





Preparing for Your CMMC Interview: Commonly Asked Questions – Access Control Edition

Access Control forms the foundation for many of the CMMC practices, ensuring the security and privacy of data and resources within an organization. Its primary purpose is to regulate who or what may access specific information by implementing robust mechanisms to protect data and prevent unauthorized access. By implementing these mechanisms, organizations can ensure that only authorized individuals or systems can perform specific actions.

Key

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

Security Requirement Table of Contents

Access Control

- Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).....5
- Control CUI posted or processed on publicly accessible systems.....6
- Limit use of portable storage devices on external systems.....7
- Verify and control/limit connections to and use of external systems.....8
- Encrypt CUI on mobile devices and mobile computing platforms.....9
- Control connection of mobile devices.....10
- Protect wireless access using authentication and encryption.....12
- Authorize wireless access prior to allowing such connections.....13
- Authorize remote execution of privileged commands and remote access to security-relevant information.....14
- Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.....15
- Monitor and control remote access sessions.....16
- Route remote access via managed access control points.....17
- Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.....18
- Provide privacy and security notices consistent with applicable CUI rules.....19
- Limit unsuccessful logon attempts.....20
- Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.....22
- Use non-privileged accounts or roles when accessing nonsecurity functions.....23
- Employ the principle of least privilege, including for specific security functions and privileged accounts..24

- Separate the duties of individuals to reduce the risk of malevolent activity without collusion.....25
- Control the flow of CUI in accordance with approved authorizations.....26
- Limit system access to the types of transactions and functions that authorized users are permitted to execute.....27
- Terminate (automatically) a user session after a defined condition.....28

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?



Access Control

AC.L1-3.1.1

Basic

Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

- How are user access privileges determined and assigned?
- How do you ensure that only authorized users have access to your systems?
- How often do you review and update user access privileges?
- Describe the process for revoking access when an employee leaves the company or changes roles.
- How are processes authenticated before they are granted access to resources?
- How do you ensure that processes only have the minimum necessary permissions to perform their tasks?
- How do you monitor and log process activities on your systems?
- How do you ensure that only authorized devices can connect to your network or systems?
- Do you have a device management policy in place?
- How do you handle lost or stolen devices?
- How do you manage and secure remote access to your systems?
- What authentication methods are in place for remote access?
- Are there any additional security layers (e.g., VPN, multi-factor authentication) in place for remote access?
- How do you monitor and log access to your systems?
- How often do you review access logs?
- Describe any incidents where unauthorized access was detected and how it was handled.
- How do you train your employees about the importance of access control?
- Are there any penalties or consequences for employees who violate access control policies?
- How do you manage access for third parties (e.g., vendors, contractors)?
- Are third-party access requirements different from internal access requirements?:
- How do you prevent unauthorized physical access to systems and data centers?
- Do you have security measures like biometric authentication, CCTV, and alarms in place?
- What access control systems or software do you use?
- How do you ensure these systems are regularly updated and patched?

- Do you have an incident response plan in place for breaches of access control?
- Can you provide examples of past incidents and how they were managed?
- Can you provide documentation of your access control policies and procedures?
- How often are these policies reviewed and updated?
- How do you ensure that backup systems are also protected by access controls?
- Describe the process for restoring data and who has access during the recovery process.
- How do you manage access control in redundant or failover systems?



Access Control

AC.L1-3.1.22

Derived

Control CUI posted or processed on publicly accessible systems.

- How do you define and categorize CUI within your organization?
- Can you provide a list of the types of CUI that your organization handles?
- How do you identify and catalog publicly accessible systems within your organization?
- What measures are in place to prevent accidental exposure of CUI on these systems?
- How do you ensure that CUI is only accessible to authorized users even on publicly accessible systems?
- Describe the process for granting and revoking access to CUI on these systems.
- How is CUI marked or labeled to indicate its sensitivity?
- Are there automated mechanisms in place to detect and label CUI?
- How do you monitor access to CUI on publicly accessible systems?
- How long are logs retained, and who has access to these logs?
- How is CUI encrypted when stored or processed on publicly accessible systems?
- Describe the encryption standards and protocols you use.
- Do you have an incident response plan specifically for breaches involving CUI on publicly accessible systems?
- Can you provide examples of past incidents involving CUI and how they were managed?
- How do you train employees about the importance of protecting CUI, especially on publicly accessible systems?
- Are employees tested on their understanding of CUI protection measures?

- How do you ensure that third parties (e.g., vendors, contractors) understand and adhere to your CUI protection policies when interacting with your publicly accessible systems?
- Can you provide documentation of your policies and procedures related to CUI on publicly accessible systems?
- How often are these policies reviewed and updated?
- Do you have content filtering or data loss prevention (DLP) solutions in place to detect and prevent CUI from being posted or processed on publicly accessible systems?
- How do you ensure backups of CUI are also protected, especially if they are stored on or accessible from publicly accessible systems?
- How often do you conduct audits or reviews to ensure CUI is not inadvertently exposed on publicly accessible systems?
- Can you share results from the most recent audit or review?



Access Control

AC.L2-3.1.21

Derived

Limit use of portable storage devices on external systems.

- What is your organization's policy on the use of portable storage devices on external systems?
- How frequently are these policies reviewed and updated?
- How do you control which portable storage devices can be used on external systems?
- Do you have a whitelist or blacklist of approved or disallowed devices?
- Are portable storage devices encrypted when used on external systems? If so, what encryption standards are used?
- How do you ensure the security of data transferred to and from portable storage devices?
- Do you have mechanisms in place to monitor and log when portable storage devices are connected to external systems?
- How long are these logs retained, and who has access to them?
- How are employees made aware of the risks and policies associated with using portable storage devices on external systems?
- Are there penalties or consequences for violating these policies?
- Do you have a specific incident response plan for security incidents involving portable storage devices on external systems?

- Can you provide examples of past incidents and how they were addressed?
- How do you track and manage portable storage devices within your organization?
- How do you handle lost or stolen devices?
- How do you ensure that third parties, contractors, or remote workers adhere to your policies on portable storage devices on external systems?
- Do you have DLP solutions in place to detect and prevent unauthorized data transfers to portable storage devices?
- What is your procedure for securely disposing of or repurposing portable storage devices?
- How often do you audit the use of portable storage devices on external systems to ensure compliance with organizational policies?
- Can you share findings from the most recent audit or review related to this?
- How do you ensure physical security of portable storage devices when not in use?
- Do you have designated secure storage areas for these devices?
- Do you use software restrictions or endpoint security solutions to prevent unauthorized use of portable storage devices on external systems?



Access Control



AC.L1-3.1.20



Derived



Verify and control/limit connections to and use of external systems.

- How do you identify and catalog external systems that your organization connects to?
- What processes are in place to verify the authenticity and integrity of external systems before establishing a connection?
- How do you ensure that only authorized employees can connect to external systems?
- Describe any network segmentation or isolation practices you employ when connecting to external systems.
- How do you monitor and log connections to external systems?
- What criteria must an external system meet before it's allowed to connect to your network or systems?
- How do you handle connections to external systems that are initiated by third parties, vendors, or partners?
- Are there any automated tools or solutions in place to detect unauthorized connections to external systems?

- How do you ensure data integrity and confidentiality when transferring data to or from external systems?
- What encryption standards and protocols are used for data in transit to and from external systems?
- How frequently do you review and update the list of authorized external systems?
- Describe any multi-factor authentication processes in place for connections to high-risk or sensitive external systems.
- How do you train employees about the risks and protocols associated with connecting to external systems?
- Do you have a specific incident response plan for security incidents involving connections to external systems?
- How often do you conduct vulnerability assessments or penetration tests focusing on connections to external systems?
- Are there any restrictions or special protocols for connecting to external systems from remote locations or mobile devices?
- How do you ensure that software and applications used to connect to external systems are regularly updated and patched?
- Are there any data loss prevention (DLP) mechanisms in place to monitor data transfers to external systems?
- How do you manage and renew certificates and other cryptographic mechanisms used for connections to external systems?
- How do you evaluate the security posture of external systems, especially if they belong to a third party or vendor?



Access Control

AC.L2-3.1.19

Derived

Encrypt CUI on mobile devices and mobile computing platforms.

- What encryption standards and protocols do you use to encrypt CUI on mobile devices and platforms?
- How do you ensure that all mobile devices and platforms containing CUI are encrypted?
- How do you handle encryption keys, and what is the process for key management and renewal?
- Are there any automated tools or solutions in place to verify the encryption status of mobile devices and platforms?
- How do you handle lost or stolen mobile devices that contain CUI?
- How frequently do you audit or review the encryption status of mobile devices and platforms?

- How do you train employees about the importance and procedures of encrypting CUI on their mobile devices?
- Are employees allowed to store CUI on their personal mobile devices? If so, how do you ensure those devices are encrypted?
- How do you ensure that CUI remains encrypted during data transfers between mobile devices and other systems?
- What is the process for securely wiping or deleting CUI from mobile devices?
- How do you manage and update encryption software on mobile devices and platforms?
- Are there any additional layers of authentication required to access encrypted CUI on mobile devices?
- How do you address the risk of malware or other threats that could potentially compromise encryption mechanisms on mobile devices?
- How do you ensure third parties or contractors adhere to your encryption requirements for CUI on mobile devices?
- What measures are in place to prevent unauthorized access to encrypted CUI in the event of device compromise?
- How do you handle backups of CUI on mobile devices, and are these backups also encrypted?
- Are there any exceptions or exemptions to the encryption requirement, and how are they justified and documented?
- How do you handle updates or patches to encryption software or tools to address vulnerabilities?
- What is the procedure for employees to report issues or concerns related to encryption on their mobile devices?
- How do you evaluate and select encryption solutions for mobile devices and platforms to ensure they meet organizational and regulatory requirements?



Access Control



AC.L2-3.1.18



Derived



Control connection of mobile devices.

- How do you define “mobile devices” within your organization’s security policy?
- What policies and procedures are in place to manage the connection of mobile devices to organizational systems and networks?
- How do you ensure that only authorized mobile devices are allowed to connect to your systems and networks?

- Describe the process of onboarding a new mobile device into the system.
- How do you handle lost or stolen mobile devices? Is there a process for remotely wiping or locking such devices?
- Are mobile devices required to have endpoint protection or any specific security configurations before they can access the organizational network?
- How do you segregate personal and work data on mobile devices?
- How are software updates and patches managed on mobile devices connected to your network?
- What kind of encryption standards are implemented for data at rest and in transit on mobile devices?
- Are there any restrictions on types or models of mobile devices that can connect to the organizational network?
- How do you ensure that mobile devices do not connect to unsecured or unauthorized networks when outside the organization?
- How do you handle the decommissioning or offboarding of mobile devices from the system?
- Are users trained on the security risks associated with mobile devices and best practices to mitigate those risks?
- Describe any Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) solutions in place.
- How do you monitor and log the activities of mobile devices connected to your network?
- Are there any geographic or location-based restrictions for connecting mobile devices to the organizational network?
- How do you ensure that mobile applications installed on devices are secure and free from malicious software?
- How frequently do you audit the mobile devices connected to your network to ensure compliance with organizational policies?
- What measures are in place to prevent data leakage or unauthorized data transfer from mobile devices?
- How do you handle incidents related to mobile device security breaches or vulnerabilities?



Access Control



AC.L2-3.1.17



Derived



Protect wireless access using authentication and encryption

- What wireless protocols and standards are currently in use within your organization (e.g., WPA2, WPA3)?
- Describe the authentication methods used for wireless access. Are they based on something the user knows (password), has (token or smart card), or is (biometric)?
- How do you ensure the strength and security of wireless access passwords or passphrases?
- Are multi-factor authentication (MFA) methods employed for wireless access?
- Describe the encryption protocols implemented for wireless data transmission.
- How frequently are encryption keys rotated or changed?
- How do you handle the distribution and storage of pre-shared keys (PSK) for wireless access?
- Are there separate wireless networks or SSIDs for guests, internal users, and IoT devices?
- How do you ensure that wireless access points (WAPs) are securely configured and regularly updated?
- Describe any wireless intrusion detection or prevention systems (WIDS/WIPS) in place.
- How do you handle the detection of rogue wireless access points or devices?
- Are there any policies or procedures for users connecting personal wireless devices to the network?
- How do you ensure the physical security of wireless access points to prevent tampering or unauthorized access?
- Describe any segmentation or isolation practices for devices connected via wireless networks.
- How frequently do you perform wireless security assessments or penetration tests?
- How do you handle the decommissioning or replacement of outdated or vulnerable wireless equipment?
- Are there any geographic or location-based restrictions for setting up wireless access points?
- How do you ensure the ongoing confidentiality and integrity of data transmitted over wireless networks?
- Are users trained on the security risks associated with wireless connections and best practices to mitigate those risks?
- What incident response procedures are in place for potential breaches or vulnerabilities associated with wireless networks?



Access Control



AC.L2-3.1.16



Derived



Authorize wireless access prior to allowing such connections

- How do you determine who or what is authorized to connect to your wireless network?
- Describe the process for granting authorization for wireless access.
- What systems or tools do you use to manage and monitor wireless access authorizations?
- How do you handle requests for temporary or guest wireless access?
- Are there any automated systems in place to grant or revoke wireless access based on predefined criteria?
- How do you ensure that unauthorized devices do not gain access to your wireless network?
- What measures are in place to detect and respond to unauthorized wireless connections?
- How frequently do you review and update the list of authorized wireless devices and users?
- How do you handle the decommissioning or removal of devices or users from the authorized list?
- Describe any role-based access controls (RBAC) in place for wireless access.
- Are there different levels or tiers of wireless access authorization based on user roles or device types?
- How do you ensure that wireless access rights are in alignment with job functions or business requirements?
- How are changes to wireless access authorization documented and communicated?
- How do you handle the renewal or expiration of wireless access authorizations?
- Describe any Mobile Device Management (MDM) or similar solutions in place that assist with wireless access authorization.
- What criteria or standards must a device meet to be eligible for wireless access authorization?
- How do you handle wireless access for third-party or external entities such as vendors or contractors?
- What training or awareness programs are in place to educate users about wireless access authorization protocols?
- How do you ensure that revoked or expired authorizations do not gain wireless access?
- Are there any periodic audits or assessments to validate the effectiveness of wireless access authorization procedures?



Access Control

AC.L2-3.1.15

Derived

Authorize remote execution of privileged commands and remote access to security-relevant information.

- How do you determine who is authorized to remotely execute privileged commands?
- What systems or tools are in place to manage and monitor remote execution of privileged commands?
- Describe the process for granting and revoking authorization for remote execution of privileged commands.
- How do you ensure the integrity and authenticity of commands being executed remotely?
- Are there any specific protocols or encryption standards used for the transmission of privileged commands?
- How do you log and monitor the remote execution of privileged commands?
- Describe the process for granting access to security-relevant information remotely.
- What criteria or standards must a user meet to be eligible for remote access to security-relevant information?
- How do you ensure the confidentiality and integrity of security-relevant information accessed remotely?
- Are multi-factor authentication (MFA) methods employed for remote execution of privileged commands or access to security-relevant information?
- How do you handle requests for temporary or emergency remote execution of privileged commands?
- How frequently do you review and update the list of authorized users for remote privileged command execution and access to security-relevant information?
- Describe any role-based access controls (RBAC) in place for this practice.
- How do you ensure that users with these privileges are adequately trained and aware of the responsibilities?
- Are there any automated systems in place to detect and alert on unauthorized or suspicious remote privileged activities?
- How do you handle incidents related to unauthorized remote execution of privileged commands or unauthorized access to security-relevant information?
- How do you validate the need for users to have the capability to execute privileged commands remotely?
- Are there any geographic or location-based restrictions or additional security layers for users attempting to execute privileged commands or access security-relevant information remotely?

- How do you handle third-party or vendor access related to remote privileged command execution or access to security-relevant data?
- Are there periodic audits or assessments to validate the effectiveness of controls related to remote execution of privileged commands and access to security-relevant information?



Access Control



AC.L2-3.1.13



Derived



Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

- What cryptographic algorithms and protocols are used to secure remote access sessions?
- How do you ensure that the cryptographic mechanisms in use align with current best practices and recommendations?
- Describe the process of key management, including generation, distribution, storage, and retirement.
- How frequently are cryptographic keys rotated or changed?
- Are there any specific requirements or standards for cryptographic strength (e.g., key lengths) in the context of remote access?
- How do you handle the detection and mitigation of weak or deprecated cryptographic protocols and ciphers?
- Describe the process for updating or upgrading cryptographic mechanisms in response to emerging threats or vulnerabilities.
- How do you ensure that remote access solutions (e.g., VPNs, remote desktop tools) employ secure cryptographic mechanisms by default?
- Are there any mechanisms in place to prevent man-in-the-middle attacks during remote access sessions?
- How do you ensure that end-users and remote devices employ the necessary cryptographic protections before initiating a remote access session?
- Do you employ mutual authentication mechanisms during remote access to ensure both the client and server sides are legitimate?
- Are there specific cryptographic requirements for third-party or external entities when they require remote access?
- How do you validate the effectiveness and integrity of the cryptographic protections on remote access sessions?
- How do you handle incidents where the cryptographic protections of a remote access session may have been compromised?

- Are users trained on the importance and role of cryptographic protections during remote access?
- Do you have logging and monitoring in place to detect potential cryptographic anomalies or failures during remote access sessions?
- How do you ensure that backup or redundant remote access systems also adhere to the required cryptographic standards?
- Are there periodic reviews or assessments to validate the effectiveness of cryptographic mechanisms for remote access?
- How do you handle the deprecation of cryptographic standards or protocols in the context of remote access?
- Are there any additional layered security measures employed in conjunction with cryptographic protections for remote access?



Access Control

AC.L2-3.1.12

Derived

Monitor and control remote access sessions.

- What tools and systems are in place to monitor remote access sessions in real-time?
- How do you identify and authenticate users before granting remote access?
- Describe the logging mechanisms for remote access sessions. What information is recorded?
- How long are logs for remote access sessions retained, and who has access to them?
- What measures are in place to detect unauthorized or suspicious remote access attempts?
- How do you respond to detected unauthorized remote access sessions or anomalies?
- Describe any automated systems in place for alerting or blocking certain remote access behaviors.
- Are there any time-based restrictions on remote access, such as allowable connection times or session durations?
- How do you ensure the integrity of data during remote access sessions?
- Are there any geographic or location-based controls for remote access? For example, are users restricted from accessing remotely from certain countries?
- How do you handle simultaneous remote access sessions from the same user credentials?
- What measures are in place to prevent data exfiltration during remote access sessions?
- Describe any session timeout or automatic disconnection policies for remote access.
- How frequently do you review logs and reports related to remote access sessions?

- How do you validate and ensure that remote access sessions terminate correctly and completely?
- Are there specific bandwidth or connection quality requirements for remote access sessions?
- Describe any role-based access controls (RBAC) in place that might limit or dictate remote access capabilities.
- How do you educate users about the importance of proper remote access behavior and session termination?
- Are there periodic assessments or audits to validate the effectiveness of remote access session monitoring and controls?
- How do you handle third-party or vendor remote access in terms of monitoring and control?



Access Control

AC.L2-3.1.14

Derived

Route remote access via managed access control points.

- Describe the managed access control points implemented for remote access.
- How do you ensure that all remote access is directed exclusively through these managed access control points?
- What security measures are implemented at these managed access control points?
- How do you monitor and log traffic passing through these control points?
- Are there any redundancies in place for these managed access control points to ensure continuous availability?
- Describe any authentication and authorization mechanisms in place at these control points.
- How do you handle the detection of unauthorized remote access attempts that bypass these control points?
- What network segmentation or isolation practices are in place concerning these managed access control points?
- How frequently are the configurations of these access control points reviewed and updated?
- Do these managed access control points have the capability to block or terminate sessions based on predefined criteria?
- How do you ensure the security and timely patching of the software or hardware used in these control points?
- Are there any intrusion detection or prevention systems (IDPS) implemented at these control points?

- Describe any VPN gateways, proxies, or other similar technologies employed as part of these managed access control points.
- How do you manage and rotate cryptographic keys and certificates associated with these control points?
- Are there specific bandwidth or throughput limitations at these managed access control points?
- How do you test the resilience and security of these managed access control points against potential cyber attacks?
- How do you handle the addition of new managed access control points or the decommissioning of old ones?
- Are users or administrators trained on the importance and function of these managed access control points?
- Describe any rate limiting, Quality of Service (QoS), or other traffic management measures at these control points.
- How do you ensure continuous monitoring and alerting for any anomalies or issues at these managed access control points?



Access Control



AC.L2-3.1.10



Derived



Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity

- How do you implement session locks across different systems and devices in the organization?
- After what duration of inactivity is the session lock activated?
- Describe the pattern-hiding displays used during the session lock. How do they obscure or hide on-screen information?
- How do you ensure that all workstations, laptops, and mobile devices comply with the session lock requirement?
- What is the process for users to unlock their sessions? Is multi-factor authentication required?
- How do you handle exceptions or exclusions for specific systems or applications that might have different requirements?
- How do you ensure the session lock feature isn't disabled or bypassed by end users?
- Are there any monitoring or logging mechanisms in place to detect failures or bypass attempts of the session lock feature?
- How do you educate and train users about the importance and use of session locks?

- Describe any policies or procedures in place that mandate the use of session locks with pattern-hiding displays.
- Are there automated tools or solutions employed to enforce and verify the session lock settings across the organization's devices?
- How do you handle third-party applications or systems that may not natively support pattern-hiding displays during session locks?
- How frequently do you audit or assess the effectiveness and compliance of the session lock feature across the organization?
- How do you handle incidents or reports of session locks being compromised or bypassed?
- Are there any additional security measures in place, in conjunction with session locks, to enhance data protection during inactivity?
- How do you ensure that remote or off-site devices, especially those used by remote workers, comply with the session lock requirements?
- Describe any customizations or configurations applied to the default session lock settings based on specific roles or departments.
- How do you test and validate the effectiveness of pattern-hiding displays in obscuring on-screen data?
- Are there any exemptions from this requirement based on user roles or system criticality?
- How do you ensure that updates or changes to the IT environment don't inadvertently affect the functionality of session locks with pattern-hiding displays?



Access Control

AC.L2-3.1.9

Derived

Provide privacy and security notices consistent with applicable CUI rules.

- How do you ensure that privacy and security notices are in line with current CUI requirements?
- Where are these privacy and security notices displayed or communicated to users?
- How frequently do you review and update your privacy and security notices?
- Who within the organization is responsible for drafting and approving these notices?
- Describe the process for integrating feedback or changes from regulatory bodies into your privacy and security notices.
- How do you ensure all stakeholders, including employees, contractors, and third parties, are aware of the latest privacy and security notices?
- Are there training programs or awareness campaigns centered around these privacy and security notices?

- How do you handle discrepancies or conflicts between organizational policies and CUI rules in these notices?
- How are these notices tailored or adapted for different platforms or mediums (e.g., web, mobile, print)?
- Describe any mechanisms in place to ensure users actively acknowledge or consent to these notices.
- How do you ensure that the privacy and security notices are clear, understandable, and not misleading?
- How do you address multi-jurisdictional challenges, if any, in your privacy and security notices with respect to CUI rules?
- Are users provided with channels or methods to seek clarifications or raise concerns about these notices?
- How do you archive or maintain historical versions of these privacy and security notices?
- Describe any incident response plans in place should there be a violation or non-compliance with the stated privacy and security notices.
- How do you ensure external systems or third-party integrations align with the stated privacy and security notices related to CUI?
- Are there periodic audits or assessments to validate the consistency and compliance of these notices with CUI rules?
- How do you handle updates or changes to CUI rules and their subsequent impact on your privacy and security notices?
- Are there specific departments or roles within the organization that are exempt from certain aspects of these notices?
- How do you ensure that the privacy and security notices are accessible and inclusive to all users, including those with disabilities?



Access Control



AC.L2-3.1.8



Derived



Limit unsuccessful logon attempts.

- How many unsuccessful logon attempts are allowed before action is taken?
- What actions are taken after the threshold of unsuccessful logon attempts is reached?
- How do you track and log unsuccessful logon attempts across different systems and applications?
- Are there different thresholds or actions for different types of accounts (e.g., user accounts vs. administrator accounts)?
- How long does an account remain locked or restricted after reaching the threshold of unsuccessful logon attempts?

- Describe the process for users to unlock their accounts or reset their credentials after being locked out.
- How do you handle potential brute-force attacks or multiple unsuccessful logon attempts from different sources?
- Are there alerts or notifications set up to inform administrators or security teams of multiple unsuccessful logon attempts?
- How do you ensure that the mechanisms for limiting unsuccessful logon attempts are consistently applied across all systems, applications, and platforms?
- How do you educate users about the importance of security practices related to logon attempts?
- Are there any exemptions or special rules for critical accounts or systems concerning unsuccessful logon attempts?
- How frequently do you review and update policies and configurations related to limiting unsuccessful logon attempts?
- How do you handle false positives, such as legitimate users being locked out due to unintentional mistakes?
- Are there monitoring tools or solutions in place to analyze patterns or trends in unsuccessful logon attempts?
- How do you address the risk of Denial of Service (DoS) attacks related to account lockouts?
- Are users provided with feedback or guidance when they approach the threshold of unsuccessful logon attempts?
- Describe any multi-factor authentication (MFA) or additional security layers employed in conjunction with or after multiple unsuccessful logon attempts.
- How do you handle third-party or external system logon attempts in terms of unsuccessful attempt thresholds?
- Are there periodic assessments or tests to validate the effectiveness of controls related to limiting unsuccessful logon attempts?
- How do you ensure that updates or system changes don't inadvertently affect the functionality related to limiting unsuccessful logon attempts?



Access Control

AC.L2-3.1.7

Derived

Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

- How do you define privileged functions within your organization's systems and applications?
- Describe the mechanisms in place to restrict non-privileged users from executing privileged functions.
- How are user roles and privileges assigned and managed within the organization?
- What systems or tools are in place to monitor and log the execution of privileged functions?
- How do you handle attempts by non-privileged users to execute privileged functions?
- How frequently do you review and update user roles and privileges to ensure they align with job responsibilities?
- Describe the structure and content of the audit logs related to the execution of privileged functions.
- How long are audit logs retained, and who has access to them?
- What alerts or notifications are set up to inform of unauthorized attempts at executing privileged functions?
- How do you ensure that the audit logs themselves are protected from tampering or unauthorized access?
- Are there any mechanisms in place to detect and alert on privilege escalation attempts?
- How do you educate users about the importance of adhering to their designated privileges?
- How do you handle third-party or vendor access in terms of privileged functions?
- Are there periodic reviews or audits to verify that only appropriate users have access to privileged functions?
- Describe any incident response plans or procedures in place for situations where non-privileged users execute privileged functions.
- How do you ensure consistency in role-based access controls (RBAC) across different systems, platforms, and applications?
- How do you test and validate the effectiveness of controls related to privileged function execution?
- Describe any automated systems or solutions employed to manage and monitor privileged function access and execution.
- How do you handle the onboarding and offboarding of users in relation to privileged functions?
- Are there specific protocols or additional security measures for logging privileged functions executed during emergency or exceptional scenarios?



Access Control



AC.L2-3.1.6



Derived



Use non-privileged accounts or roles when accessing nonsecurity functions

- How do you differentiate between privileged and non-privileged accounts within your systems and applications?
- Describe the mechanisms in place to ensure users utilize non-privileged accounts when accessing nonsecurity functions.
- How do you educate and train users about the importance of using appropriate account levels for their tasks?
- What systems or tools are in place to monitor and detect instances where privileged accounts are used for nonsecurity functions?
- How do you handle violations or instances where privileged accounts are used inappropriately?
- Are users provided with both privileged and non-privileged accounts, based on their roles and responsibilities?
- How frequently do you review and audit user actions to ensure compliance with this practice?
- How do you ensure third-party or vendor personnel follow this practice when accessing your systems?
- What mechanisms are in place to automatically enforce or remind users to switch to non-privileged accounts for nonsecurity tasks?
- Are there alerts or notifications set up to inform administrators or security teams of inappropriate account usage?
- How do you define nonsecurity functions within your systems and applications?
- Describe any access controls, such as role-based access controls (RBAC), implemented to enforce this practice.
- How do you handle exceptions or scenarios where privileged accounts might be required for nonsecurity functions?
- How do you ensure that the controls and policies related to this practice are consistently applied across all systems and platforms?
- What is the process for users to request elevated privileges if required temporarily?
- How do you ensure that users revert to non-privileged accounts after completing tasks that required elevated privileges?
- Are there periodic training or awareness programs to reinforce the importance of this practice among users?

- How do you manage and monitor account privileges, especially for users with dynamic roles or responsibilities?
- Are there periodic assessments or tests to validate the effectiveness of controls related to this practice?
- How do you handle and respond to feedback or concerns from users regarding account privilege restrictions?



Access Control



AC.L2-3.1.5



Derived



Employ the principle of least privilege, including for specific security functions and privileged accounts.

- How do you define and implement the principle of least privilege within your organization?
- Describe the process for assigning privileges to user accounts. How do you determine the minimum necessary access for each role?
- How do you handle requests for elevated privileges or exceptions to the principle of least privilege?
- What systems or tools are in place to monitor and enforce the principle of least privilege across different systems and applications?
- How frequently do you review user privileges and permissions to ensure alignment with their roles and responsibilities?
- Describe the controls in place for privileged accounts. How do you ensure they are not used for routine tasks?
- How do you educate and train users about the importance of the principle of least privilege?
- How do you manage temporary elevation of privileges, and how do you ensure such privileges are revoked after the need is addressed?
- Are there specific audit trails or logs maintained for actions taken by privileged accounts?
- How do you handle third-party or vendor access in relation to the principle of least privilege?
- What mechanisms are in place to automatically enforce or remind users to operate with the least amount of privilege necessary?
- Are there alerts or notifications set up to inform administrators or security teams of potential violations of the principle of least privilege?
- Describe any role-based access controls (RBAC) or attribute-based access controls (ABAC) implemented to support the principle of least privilege.
- How do you address the risks of privilege escalation or potential misuse of elevated privileges?

- How do you ensure the principle of least privilege is applied consistently across various platforms, applications, and environments (e.g., cloud, on-premises)?
- Are there periodic assessments or tests to validate the effectiveness of controls related to the principle of least privilege?
- How do you handle and respond to incidents where excessive privileges were used or exploited?
- How do you ensure newly deployed systems, applications, or services adhere to the principle of least privilege by default?
- Are there specific procedures or controls for critical or sensitive systems to further enforce the principle of least privilege?
- How do you manage the lifecycle of accounts, especially in relation to changing roles, departures, or transfers, to maintain adherence to the principle of least privilege?



Access Control

AC.L2-3.1.4

Derived

Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

- How do you define and implement the concept of separation of duties within your organization?
- What processes or systems do you have in place to ensure that no single individual has control over all aspects of any critical transaction?
- Describe roles within your organization that are particularly sensitive, and how duties are separated among them.
- How do you handle roles or tasks that require elevated or privileged access in relation to the separation of duties?
- Are there automated controls in place to enforce separation of duties, especially in critical systems or applications?
- How frequently do you review and reassess the allocation of duties to ensure effective separation?
- How do you train and educate employees about the importance and implementation of separation of duties?
- What monitoring or logging mechanisms are in place to detect potential violations or bypasses of separation of duties?
- How do you handle exceptions or situations where separation of duties might be challenging due to staffing or other constraints?
- Describe any incidents or lessons learned related to the separation of duties, and how you addressed them.

- How do you ensure third-party vendors or partners adhere to the principle of separation of duties when interacting with your systems or data?
- Are there specific tools or software solutions employed to assist in managing and enforcing separation of duties?
- How do you manage the separation of duties in relation to project management or development environments?
- What measures are in place to detect and prevent collusion between employees that might bypass the separation of duties?
- Are there periodic audits or assessments to validate the effective implementation of separation of duties?
- How do you handle role changes, transfers, or promotions in the context of maintaining an effective separation of duties?
- Are there specific procedures or guidelines for implementing separation of duties for new systems, processes, or services introduced into the organization?
- How do you ensure that backups or contingency plans maintain the integrity of the separation of duties in emergency or exceptional scenarios?
- Describe any role-based access controls (RBAC) or attribute-based access controls (ABAC) strategies employed to support the separation of duties.
- How do you manage and communicate the importance of separation of duties during onboarding or role orientation?



Access Control

AC.L2-3.1.3

Derived

Control the flow of CUI in accordance with approved authorizations.

- How do you identify and categorize CUI within your organization's systems and networks?
- Describe the processes and controls in place to manage the flow of CUI.
- How do you ensure that the transfer or flow of CUI is in accordance with approved authorizations?
- What mechanisms are in place to monitor and log the movement or transfer of CUI?
- How do you manage requests for new authorizations related to the flow of CUI?
- How do you handle situations where CUI is transferred without the necessary authorizations?
- Are there specific tools or solutions employed to enforce and verify CUI flow controls?

- How do you train and educate employees about the importance of managing CUI in line with approved authorizations?
- How do you ensure that third-party vendors or partners adhere to the approved authorizations when handling CUI?
- How frequently do you review and reassess authorizations related to the flow of CUI?
- Describe any encryption or protection measures used during the transfer or flow of CUI.
- How do you handle retention and disposal of CUI in relation to approved authorizations?
- Are there alerts or notifications set up to inform of potential unauthorized flows of CUI?
- How do you ensure that backups, replicas, or copies of CUI also adhere to the flow controls and approved authorizations?
- How do you handle incidents or breaches related to the unauthorized flow of CUI?
- Are there periodic audits or assessments to validate the effective control of CUI flows in accordance with authorizations?
- How do you manage the lifecycle of CUI, especially when its classification or authorization requirements change?
- Describe any network segmentation, isolation, or other architectural considerations implemented to control CUI flows.
- How do you address the flow of CUI in cloud environments or other external platforms?
- How do you ensure continuity and compliance in controlling CUI flows during system upgrades, migrations, or other major IT changes?



Access Control



AC.L1-3.1.2



Basic



Limit system access to the types of transactions and functions that authorized users are permitted to execute.

- How do you determine and define the types of transactions and functions each user role is authorized to execute?
- What mechanisms are in place to enforce these access limitations based on user roles and authorizations?
- Describe the process for reviewing and updating user authorizations for specific transactions and functions.
- How do you handle requests for additional access or exceptions to the established access controls?
- How do you monitor and log user activities to ensure they are only performing authorized transactions and functions?

- How do you educate and inform users about their access limitations and authorized tasks?
- What measures are in place to detect and respond to unauthorized attempts to access or execute transactions and functions?
- Are there specific tools or software solutions you use to manage and enforce these access limitations?
- How frequently do you review and audit user activities to ensure compliance with their authorized access?
- How do you manage third-party or vendor access in terms of authorized transactions and functions?
- Describe any role-based access controls (RBAC) or attribute-based access controls (ABAC) strategies employed to enforce these limitations.
- How do you ensure that system updates, changes, or migrations don't inadvertently change or compromise these access controls?
- Are there alerts or notifications set up to inform administrators or security teams of potential violations of access limitations?
- How do you handle and respond to incidents where users have accessed or executed transactions or functions beyond their authorizations?
- How do you manage the onboarding and offboarding of users to ensure they are only granted access to appropriate transactions and functions?
- Describe any multi-factor authentication (MFA) or additional security layers employed in conjunction with these access limitations.
- How do you test and validate the effectiveness of controls related to limiting system access to authorized transactions and functions?
- How do you ensure that backup or contingency systems also adhere to these access limitations?
- How do you address the challenge of maintaining these access controls in dynamic or rapidly changing environments, such as DevOps or agile settings?
- How do you ensure that separation of duties is maintained while implementing these access controls?



Access Control



AC.L2-3.1.11



Derived



Terminate (automatically) a user session after a defined condition.

- How frequently do you review or audit your processes related to this standard?

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

Preparing for Your CMMC Interview: Commonly Asked Questions – Audit and Accountability Edition

The primary function of this domain is to systematically monitor and review actions and events that occur within a system or network. This assures that all operations, including those involving sensitive data, are traceable to an individual or component. By maintaining these detailed records, organizations can not only identify discrepancies, irregularities, or other issues – these detailed records ensure accountabilities for all actions within an organization.

For example, imagine a CCTV. If something goes wrong, you can review the footage to find out what happened. This family ensures that actions are logged and traceable, helping to spot and investigate any mishaps.

Key

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

Security Requirement Table of Contents

Audit and Accountability

- Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.....4
- Limit management of audit logging functionality to a subset of privileged users.....5
- Protect audit information and audit logging tools from unauthorized access, modification, and deletion.....6
- Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.....7
- Provide audit record reduction and report generation to support on-demand analysis and reporting.....8
- Alert in the event of an audit logging process failure.....9
- Review and update logged events.....10
- Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.....11
- Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.....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?



Audit and Accountability

AU.L2-3.3.5

Derived

Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

- How do you collect and correlate audit records across different systems, applications, and platforms?
- Describe the processes in place for regular review and analysis of audit records.
- What tools or software solutions do you use for audit record correlation and analysis?
- How do you define and categorize “unlawful,” “unauthorized,” “suspicious,” or “unusual” activities within your audit logs?
- What thresholds or criteria trigger an in-depth investigation based on audit records?
- How do you ensure timely reporting and escalation of suspicious activities identified from audit records?
- Describe the workflow from the detection of an unusual activity in audit records to the final resolution or mitigation.
- How do you integrate and correlate audit records with other security information and event management (SIEM) systems or threat intelligence feeds?
- How frequently do you review and update the criteria or definitions for suspicious or unauthorized activities in audit records?
- How do you handle false positives or benign activities that might be flagged as suspicious in audit records?
- How do you train and educate your team on the processes for audit record review, analysis, and correlation?
- Are there automated alerts or notifications set up based on specific patterns or anomalies in audit records?
- How do you ensure data integrity and prevent tampering with audit records?
- How do you manage the retention and storage of audit records, especially considering potential future investigations?
- Describe any incident response drills or exercises you conduct based on indications from audit records.
- How do you collaborate with external entities, such as law enforcement or other organizations, based on findings from audit records?
- How do you incorporate lessons learned from past incidents into the audit record review and correlation processes?

- Are there specific challenges or considerations in correlating audit records in hybrid or multi-cloud environments?
- How do you ensure that third-party vendors or integrated systems adhere to the same standards for audit record generation and correlation?
- How do you prioritize and manage the vast volume of audit records, especially in large or complex environments?



Audit and Accountability



AU.L2-3.3.9



Derived



Limit management of audit logging functionality to a subset of privileged users.

- How do you define and identify the subset of privileged users authorized to manage audit logging functionality?
- What controls are in place to ensure only this subset of users can access and manage audit logs?
- How do you handle requests for access or modifications to audit logging functionality outside of this subset of privileged users?
- Describe the training or awareness programs in place for the subset of users responsible for managing audit logging.
- How do you monitor and log activities of these privileged users when they access or modify audit logging functionality?
- What mechanisms are in place to detect and alert on unauthorized access or modifications to audit logging functions?
- How do you ensure the integrity and tamper-proof nature of audit logs, even when accessed by privileged users?
- How frequently do you review and update the list of privileged users with access to audit logging management?
- Are there specific tools or software solutions you use to enforce and monitor access to audit logging functionality?
- How do you handle the onboarding and offboarding of privileged users in relation to audit logging management?
- Describe any role-based access controls (RBAC) or attribute-based access controls (ABAC) strategies employed to enforce this limited access.
- Are there periodic audits or assessments to validate that only the defined subset of privileged users can manage audit logging?

- How do you handle backups, archives, or migrations of audit logs, and who has access to these processes?
- How do you segregate duties among the subset of privileged users to ensure no single individual has unchecked authority over audit logging?
- How do you ensure that third-party vendors or integrated systems adhere to the same standards for audit logging management access?
- Describe any incident response plans or procedures in place for situations where unauthorized access to audit logging functionality is detected.
- How do you manage access to audit logging functionality in distributed or remote environments?
- How do you ensure continuity and compliance in limiting access to audit logging functions during system upgrades, migrations, or other major IT changes?
- Are there specific challenges or considerations in managing access to audit logging functions in hybrid or multi-cloud environments?
- How do you address the risk of insider threats or potential misuse of access by the subset of privileged users?



Audit and Accountability

AU.L2-3.3.8

Derived

Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

- What controls are in place to restrict unauthorized access to audit information and logging tools?
- How do you ensure the integrity of audit logs to prevent unauthorized modifications?
- Describe the mechanisms used to safeguard audit logs against unauthorized deletion.
- What tools or software solutions do you employ to monitor and protect access to audit logging tools?
- How do you handle backups or archives of audit logs to ensure they remain protected?
- How do you ensure that third-party vendors or external entities do not have unauthorized access to audit information?
- Are there any encryption measures applied to audit logs, especially during storage or transmission?
- How do you detect and respond to incidents of unauthorized access, modification, or deletion of audit logs?
- How frequently do you review and update the access controls related to audit information and logging tools?

- Describe any role-based access controls (RBAC) or attribute-based access controls (ABAC) strategies employed to protect audit logs.
- How do you train and inform employees about the importance of protecting audit logs and the tools associated with them?
- How do you ensure the continuity of audit log protection during system updates, migrations, or other IT changes?
- Are there specific challenges or considerations in protecting audit logs in hybrid or multi-cloud environments?
- How do you ensure that audit logging tools themselves are up-to-date and protected from vulnerabilities or exploits?
- Are there periodic audits or assessments to validate the protection measures in place for audit logs and tools?
- How do you segregate duties among users to ensure no single individual has unchecked authority over audit logs or tools?
- Are there alerts or notifications set up to inform of potential threats or breaches related to audit log protection?
- Describe any incident response plans or procedures in place for situations where audit log protection is compromised.
- How do you manage retention and disposal of audit logs to ensure they remain protected throughout their lifecycle?
- How do you ensure audit logs are protected during transit, especially if they are sent to external systems or off-site locations?



Audit and Accountability

AU.L2-3.3.7

Derived

Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records

- What controls are in place to restrict unauthorized access to audit information and logging tools?
- How do you ensure the integrity of audit logs to prevent unauthorized modifications?
- Describe the mechanisms used to safeguard audit logs against unauthorized deletion.
- What tools or software solutions do you employ to monitor and protect access to audit logging tools?
- How do you handle backups or archives of audit logs to ensure they remain protected?

- How do you ensure that third-party vendors or external entities do not have unauthorized access to audit information?
- Are there any encryption measures applied to audit logs, especially during storage or transmission?
- How do you detect and respond to incidents of unauthorized access, modification, or deletion of audit logs?
- How frequently do you review and update the access controls related to audit information and logging tools?



Audit and Accountability

AU.L2-3.3.6

Derived

Provide audit record reduction and report generation to support on-demand analysis and reporting.

- How do you reduce and consolidate audit records for analysis?
- Describe the tools or software solutions you use for audit record reduction and report generation.
- How do you ensure the integrity of audit data during the reduction process?
- What criteria or filters are applied during audit record reduction to ensure relevant data is retained for analysis?
- How frequently do you generate reports from the reduced audit records?
- How do you handle on-demand requests for specific audit analyses or reports?
- Describe the types of reports that can be generated from the reduced audit records.
- How do you ensure that generated reports are protected from unauthorized access or modification?
- Are there any automated alerts or notifications set up based on specific patterns or anomalies detected during the audit record reduction?
- How do you train and educate relevant personnel on using the audit record reduction and report generation tools?
- How do you handle the retention and disposal of original audit records after reduction?
- How do you ensure that third-party systems or integrated platforms adhere to the same standards for audit record reduction and report generation?
- How do you validate the accuracy and completeness of reports generated from reduced audit records?
- Describe any challenges or considerations you've encountered in audit record reduction, and how you've addressed them.

- Are there periodic reviews or audits to validate the effectiveness of the audit record reduction and report generation processes?
- How do you manage and prioritize on-demand requests for audit analysis or reports?
- How do you ensure continuity in audit record reduction and report generation during system updates, migrations, or other IT changes?
- How do you handle feedback or concerns related to the generated reports or the reduction process?
- Are there specific mechanisms in place to handle large or complex datasets during the audit record reduction process?
- How do you ensure that audit record reduction and report generation processes align with the organization's broader cybersecurity and compliance goals?



Audit and Accountability

AU.L2-3.3.4

Derived

Alert in the event of an audit logging process failure.

- How do you detect failures in your auditing processes?
- What mechanisms are in place to generate alerts upon the detection of an auditing process failure?
- How are these alerts communicated to the relevant personnel or teams?
- What is the expected response time once an alert for an auditing process failure is received?
- Describe the tools or software solutions you use for monitoring and alerting related to auditing processes.
- How do you prioritize and categorize the severity of different types of auditing process failures?
- How do you train and educate relevant personnel on responding to auditing process failure alerts?
- Are there automated response actions or remedies triggered upon detection of certain auditing process failures?
- How do you ensure that third-party systems or integrated platforms also alert on auditing process failures?
- How frequently do you review and test the alerting mechanisms to ensure their effectiveness?
- Describe any incidents or lessons learned from past auditing process failures and how they were addressed.
- How do you handle false positives or benign alerts related to auditing process failures?

- How are alerts logged and documented for future analysis or review?
- Are there specific challenges or considerations you've encountered in alerting on auditing process failures, and how have you addressed them?
- How do you ensure continuity in alerting mechanisms during system updates, migrations, or other major IT changes?
- How do you collaborate with external entities, such as vendors or partners, in the event of an auditing process failure that impacts multiple parties?
- Are there periodic drills or exercises conducted to simulate auditing process failures and test the alerting and response mechanisms?
- How do you validate the accuracy and timeliness of alerts generated due to auditing process failures?
- How do you handle feedback or concerns related to the alerting mechanisms from relevant stakeholders?
- How do you ensure that the alerting mechanisms for auditing process failures align with the organization's broader cybersecurity and compliance goals?



Audit and Accountability

AU.L2-3.3.3

Derived

Review and update logged events.

- How frequently do you review logged events?
- What criteria or triggers determine when logged events need to be updated?
- Describe the tools or software solutions you use for logging, reviewing, and updating events.
- How do you ensure the integrity of logged events during the review and update process?
- Who is responsible for reviewing and updating logged events within your organization?
- What training or awareness programs are in place for personnel responsible for reviewing and updating logged events?
- How do you handle discrepancies or inconsistencies identified during the review of logged events?
- Are there any automated processes or systems in place to aid in the review and update of logged events?
- How do you ensure that third-party systems or integrated platforms also adhere to the standards for reviewing and updating logged events?
- How do you document and track changes or updates made to logged events?

- How do you handle feedback or concerns related to the review and update process of logged events?
- Are there specific challenges or considerations you've encountered in reviewing and updating logged events, and how have you addressed them?
- How do you prioritize which logged events to review, especially in large or complex systems?
- How do you ensure continuity in the review and update process during system updates, migrations, or other major IT changes?
- How do you validate the accuracy and completeness of updates made to logged events?
- Are there periodic audits or assessments to validate the review and update process of logged events?
- How do you manage and retain historical or original versions of logged events after they are updated?
- How do you ensure that the review and update processes for logged events align with the organization's broader cybersecurity and compliance goals?
- Are there alerts or notifications set up to inform of potential issues or requirements related to the review and update of logged events?
- How do you collaborate with external entities, such as vendors or partners, in the event of a logged event that impacts multiple parties and requires coordinated review and update?



Audit and Accountability

AU.L2-3.3.2

Basic

Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.

- How do you uniquely identify each system user within your organization's infrastructure?
- What mechanisms are in place to ensure every action or transaction by a user is traceable back to them?
- How do you manage and store logs that capture user-specific actions?
- Describe the authentication and identification mechanisms you use to ensure user accountability.
- How do you handle shared accounts or roles in the context of ensuring individual accountability?
- What tools or software solutions do you employ to monitor and log user-specific actions?
- How do you handle scenarios where a user denies performing a specific action that was traced back to them?
- How do you educate and inform users about the importance of individual accountability for their actions?
- How do you ensure that third-party vendors or partners accessing your systems can also have their actions uniquely traced?
- Are there alerts or notifications set up to detect potential misuse or anomalies related to user actions?

- How frequently do you review user action logs to ensure accountability and traceability?
- How do you address potential vulnerabilities or threats that might allow actions to be falsely attributed to a user?
- Are there any specific challenges or considerations you've encountered in ensuring user accountability, and how have you addressed them?
- How do you manage the retention and storage of logs that ensure user accountability?
- Describe any incident response plans or procedures related to issues with tracing user actions.
- How do you handle the onboarding and offboarding of users to ensure continued traceability and accountability?
- How do you ensure user accountability in distributed or remote work environments?
- Are there periodic audits or assessments to validate the effective tracing of user actions for accountability?
- How do you handle feedback or concerns from users or stakeholders related to accountability and traceability mechanisms?
- How do you ensure that user accountability mechanisms align with the organization's broader cybersecurity and compliance goals?



Audit and Accountability

AU.L2-3.3.1

Basic

Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity

- How do you determine the extent and granularity of system activity to be logged for monitoring and analysis?
- What tools or software solutions do you use to create and manage system audit logs?
- Describe the retention policies in place for system audit logs.
- How do you ensure the integrity and tamper-resistance of stored audit logs?
- What mechanisms are in place to monitor, analyze, and investigate indications of unlawful or unauthorized system activity from the logs?
- How do you ensure that audit logs are available and accessible for investigation when needed?
- How do you train and educate relevant personnel on the processes related to audit log creation, retention, and analysis?

- Are there alerts or notifications set up based on specific patterns or anomalies detected in the audit logs?
- How do you handle scenarios where the volume of audit logs is exceptionally high or exceeds storage capacity?
- How do you ensure that third-party systems or integrated platforms also adhere to the same standards for audit log creation and retention?
- Describe any challenges or considerations you've encountered in creating and retaining audit logs, and how you've addressed them.
- How do you ensure the confidentiality and privacy of sensitive data within the audit logs?
- Are there periodic reviews or audits to validate the effectiveness of audit log creation and retention processes?
- How do you manage and retain backups or archives of audit logs to ensure their long-term availability?
- How do you ensure continuity in audit log creation and retention during system updates, migrations, or other major IT changes?
- How do you handle feedback or concerns related to the audit log creation and retention processes?
- How do you collaborate with external entities, such as law enforcement or partners, when sharing or investigating audit logs?
- Describe any incident response plans or procedures in place related to potential issues detected from audit logs.
- How do you manage the deletion or disposal of audit logs after they exceed their retention period?
- How do you ensure that the creation and retention of audit logs align with the organization's broader cybersecurity and compliance goals?

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

Preparing for Your CMMC Interview: Commonly Asked Questions – Awareness and Training Edition

Awareness and Training are pivotal components within an organization's cybersecurity framework, and are aimed at cultivating a culture of security amongst all personnel. It is intended to ensure that team members may both recognize potential threats and risks associated with their actions, but also that team members have sufficient knowledge (and practice) to act accordingly when/if an issue occurs.

Key

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

Security Requirement Table of Contents

Awareness and Training

- Provide security awareness training on recognizing and reporting potential indicators of insider threat.....4
- Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.....5
- Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.....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?



Awareness and Training

AT.L2-3.2.3

Derived

Provide security awareness training on recognizing and reporting potential indicators of insider threat.

- How frequently do you conduct security awareness training on insider threats?
- What topics or indicators are covered in your insider threat awareness training?
- How do you ensure that all employees, including contractors and temporary staff, receive this training?
- What mechanisms are in place for employees to report potential indicators of insider threats?
- How do you keep the training content updated with the latest trends and indicators related to insider threats?
- Do you utilize real-world examples or case studies during the training to illustrate potential indicators?
- What tools or platforms do you use to deliver and track completion of the insider threat awareness training?
- How do you measure the effectiveness of the insider threat awareness training?
- How do you handle employees who fail to complete or show understanding after the training?
- Are there refresher courses or follow-up sessions for employees on recognizing and reporting insider threats?
- How do you ensure that management and leadership are aligned and supportive of the insider threat awareness initiative?
- Are there any challenges or considerations you've encountered in delivering insider threat awareness training, and how have you addressed them?
- How do you address the psychological and cultural aspects of reporting potential insider threats, ensuring that employees feel safe and protected?
- How do you handle feedback or concerns from employees related to the insider threat awareness training content or process?
- Describe any incident response plans or procedures in place for handling reports of potential insider threats.
- How do you incorporate lessons learned from actual insider threat incidents into the training content?
- How do you ensure that third-party vendors or partners are aware of the indicators of insider threats related to your organization?
- Are there specific training modules or sessions for departments or roles that are more susceptible to insider threats?

- How do you collaborate with external entities or industry groups to stay updated on best practices for insider threat awareness training?
- How do you ensure that the insider threat awareness training aligns with the organization's broader cybersecurity and compliance goals?



Awareness and Training

AT.L2-3.2.2

Basic

Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

- How do you identify and define the information security-related duties and responsibilities for each role within the organization?
- What training programs are in place to equip personnel with the necessary skills and knowledge for their security-related duties?
- How frequently are these training programs conducted or updated?
- How do you ensure that new employees receive the necessary security training before undertaking their assigned duties?
- What mechanisms are in place to test or validate the effectiveness of the training provided?
- Are there refresher courses or ongoing training sessions for employees to keep them updated on security practices and protocols?
- How do you handle employees who fail to complete or show understanding after the training?
- How do you keep the training content updated with the latest security trends, threats, and best practices?
- What tools or platforms do you use to deliver and track completion of the security training?
- How do you tailor the training content to address the specific security needs and risks of different roles or departments?
- How do you ensure that third-party vendors or contractors are also trained adequately if they have security-related duties related to your organization?
- Are there any challenges or considerations you've encountered in delivering security training, and how have you addressed them?
- How do you incorporate feedback from employees or stakeholders to improve the security training content or process?
- How do you ensure that management and leadership are also adequately trained in security practices relevant to their roles?

- Describe any incident response plans or procedures that are included in the training, especially for roles directly involved in handling security incidents.
- How do you handle the transition or handover of security-related duties when employees change roles, depart, or new personnel are onboarded?
- How do you collaborate with external entities, industry groups, or security experts to enhance your security training content?
- Are there certifications, courses, or external training programs that you recommend or mandate for certain roles with critical security responsibilities?
- How do you address the dynamic nature of cybersecurity threats and ensure that training remains relevant and up-to-date?
- How do you ensure that the training provided aligns with the organization's broader cybersecurity policies, goals, and compliance requirements?



Awareness and Training

AT.L2-3.2.1

Basic

Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

- How do you communicate security risks associated with specific roles or activities to the relevant personnel?
- What methods or platforms do you use to disseminate information about applicable policies, standards, and procedures?
- How frequently do you update and communicate changes or additions to security policies and procedures?
- How do you ensure that systems administrators are kept informed of the security risks associated with their activities?
- Are there dedicated training or awareness sessions focused on security risks and the corresponding policies for managers and key personnel?
- How do you track and ensure that all users have received and acknowledged the security guidelines and procedures relevant to their roles?
- How do you address non-compliance or breaches of the communicated security procedures by any staff members?
- How do you tailor communication and awareness programs to cater to different roles, such as managers, administrators, and general users?

- How do you keep the content of these awareness programs updated with the latest security threats and best practices?
- How do you handle feedback or concerns raised by personnel related to security risks or the provided guidelines?
- How do you ensure third-party vendors, contractors, or partners are also made aware of the security risks associated with their activities and the relevant procedures?
- What mechanisms are in place for personnel to report perceived security risks or suggest improvements to existing policies?
- How do you measure the effectiveness of the awareness programs in terms of understanding and adherence to security guidelines?
- Are there any specific challenges or obstacles you've encountered in communicating security risks and procedures, and how have you addressed them?
- How do you incorporate real-world incidents or lessons learned into your awareness content to emphasize security risks?
- How do you ensure continuity in awareness and communication during organizational changes, system upgrades, or introduction of new technologies?
- How do you address the dynamic nature of cybersecurity threats and ensure continuous awareness among personnel?
- Are there periodic reviews or feedback sessions to understand the gaps or needs in security awareness programs?
- How do you collaborate with external entities or industry peers to enhance your security awareness content?
- How do you ensure that the awareness programs and communications align with the organization's broader cybersecurity objectives and NIST compliance requirements?

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

Preparing for Your CMMC Interview: Commonly Asked Questions – Configuration Management Edition

Configuration Management operates as a meticulous librarian, ensuring everything is in its proper place and that the library's systems are running smoothly. That can mean a lot of things, but in the realm of cybersecurity, it focuses on establishing and maintaining consistency of a system's performance and its functional attributes throughout the life cycle. This requires strict control of changes made to hardware, software, and other components while maintaining all baselines and documentation. Ultimately, our goal is to guard against unauthorized changes that could introduce vulnerabilities. It also aids in the quick restoration of system operations in case of disruptions.

Key

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

Security Requirement Table of Contents

Configuration Management

- Control and monitor user-installed software.....4
- Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.....5
- Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.....6
- Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.....7
- Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.....9
- Track, review, approve or disapprove, and log changes to organizational systems.....10
- Establish and enforce security configuration settings for information technology products employed in organizational systems.....11
- Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.....12
- Analyze the security impact of changes prior to implementation.....13

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?



Configuration Management

CM.L2-3.4.9

Derived

Control and monitor user-installed software.

- How do you manage permissions and rights for users to install software on organizational systems?
- What tools or solutions do you employ to monitor software installations by users?
- Describe your organization's policy regarding user-installed software. Is there a whitelist or blacklist approach?
- How do you ensure users are aware of the restrictions and guidelines related to software installation?
- What measures are in place to detect and prevent the installation of unauthorized or malicious software?
- How frequently do you audit systems for non-compliant software installations?
- How do you handle situations where non-compliant or unauthorized software is detected on a system?
- Are there alerts or notifications set up to inform IT or security teams of user-installed software in real-time?
- How do you ensure that third-party vendors or remote users adhere to the organization's guidelines on software installation?
- What training or awareness programs are in place to educate users about the risks and policies related to software installation?
- How do you handle requests from users for software that is not on the approved list?
- Describe any challenges or issues you've faced related to user-installed software and how they were addressed.
- How do you manage software licensing and compliance in the context of user-installed applications?
- How do you ensure that user-installed software does not compromise system security configurations or standards?
- Are there any specific controls or restrictions for software installation on critical or sensitive systems?
- How do you address software updates and patches for user-installed applications?
- How do you integrate the monitoring of user-installed software with other security tools or incident response systems?
- Are there periodic reviews or assessments to validate the effectiveness of controls related to user-installed software?

- How do you handle feedback or concerns from users regarding software installation policies or restrictions?
- How do you ensure that the controls and monitoring mechanisms for user-installed software align with the organization's broader cybersecurity objectives and NIST compliance requirements?



Configuration Management



CM.L2-3.4.7



Derived



Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

- How do you identify which programs, functions, ports, protocols, and services are nonessential for your organization's operations?
- What tools or solutions are in place to monitor and enforce these restrictions?
- Describe the processes in place to disable or prevent the use of identified nonessential elements.
- How do you handle exceptions or requests from users who believe they need access to a restricted program or service?
- How frequently do you review and update the list of nonessential elements to reflect changes in your organization's needs and environment?
- How do you ensure that third-party vendors or partners comply with your organization's restrictions on nonessential elements?
- Are there alerts or notifications in place to detect attempts to use or enable restricted or nonessential elements?
- How do you educate and inform staff about these restrictions and the reasons behind them?
- How do you manage updates or patches to systems without enabling previously restricted services or ports?
- What measures are in place to ensure that newly introduced systems or devices adhere to these restrictions?
- Have there been any security incidents or concerns related to nonessential programs or services in the past, and how were they addressed?
- How do you validate that disabled or restricted elements do not inadvertently affect essential operations or functionalities?
- How do you ensure that critical systems, especially those exposed to external networks, adhere strictly to these restrictions?
- How do you handle feedback or concerns from stakeholders regarding the impact of these restrictions on operations or productivity?

- Are there any challenges or considerations you've encountered in implementing these restrictions, and how have you addressed them?
- Describe any automated tools or systems in place to continuously monitor and enforce these restrictions.
- How do you test or audit the effectiveness of these restrictions in providing the desired security posture?
- How do you manage exceptions or temporary needs for certain functions or services without compromising security?
- Are there periodic reviews or assessments to validate the effectiveness of the controls in place for nonessential elements?
- How do you ensure that the restrictions on nonessential programs, functions, ports, protocols, and services align with the organization's broader cybersecurity objectives and NIST compliance requirements?



Configuration Management



CM.L2-3.4.6



Derived



Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

- How do you determine the essential capabilities required for each of your organizational systems?
- What processes are in place to configure systems to operate with the minimum set of functions necessary?
- How frequently do you review system functionalities to ensure they adhere to the principle of least functionality?
- Describe the tools or methodologies you use to enforce and verify the least functionality principle.
- How do you handle requests for additional functionalities or capabilities that go beyond the identified essentials?
- How do you ensure that third-party applications or systems integrated into your environment also adhere to the principle of least functionality?
- Are there alerts or mechanisms in place to detect deviations or attempts to expand beyond the predefined essential capabilities?
- How do you manage updates or upgrades to ensure added functionalities don't compromise the least functionality principle?
- How do you educate and inform stakeholders about the importance of operating with the minimum necessary functionalities?
- How do you address challenges or concerns related to system performance or user experience while adhering to the least functionality principle?

- Have there been any security incidents related to excessive functionalities, and how were they addressed?
- How do you ensure that systems exposed to external networks or interfaces strictly adhere to the principle of least functionality?
- Are there periodic audits or assessments to validate the adherence to the least functionality principle across systems?
- How do you handle feedback from users or departments that may feel restricted due to limited functionalities?
- How do you ensure that the principle of least functionality does not inadvertently hamper critical business processes or tasks?
- Describe any automated tools or systems in place to continuously monitor and enforce the least functionality principle.
- How do you address exceptions or specific needs that might require temporary adjustments to the principle of least functionality?
- How do you collaborate with vendors or software providers to ensure their solutions align with your least functionality requirements?
- How do you manage legacy systems or applications in the context of the least functionality principle?
- How do you ensure that the approach to least functionality aligns with the organization's broader cybersecurity objectives and NIST compliance requirements?



Configuration Management



CM.L2-3.4.5



Derived



Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

- How do you define and document access restrictions related to system changes?
- What approval processes are in place for implementing access restrictions associated with system changes?
- Describe the tools or platforms you use to enforce these access restrictions.
- How do you ensure that stakeholders are aware of and adhere to the defined access restrictions when implementing system changes?
- How frequently do you review and update the documented access restrictions to reflect changes in your organization's needs and environment?
- Are there specific protocols for emergency changes, and how do access restrictions apply in such cases?

- How do you handle exceptions or requests for temporary access beyond the documented restrictions during system changes?
- How do you audit or verify compliance with the defined access restrictions during and after system changes?
- How do you ensure that third-party vendors or partners adhere to your organization's access restrictions when involved in system changes?
- What training or awareness programs are in place to educate relevant personnel about the importance of and procedures for access restrictions during system changes?
- How do you handle non-compliance or breaches of the defined access restrictions during system changes?
- Are there alerts or notifications set up to detect unauthorized access or deviations from the restrictions during system changes?
- How do you ensure continuity and integrity of operations while enforcing access restrictions during system updates, migrations, or other changes?
- Describe any challenges or considerations you've encountered in enforcing access restrictions during system changes, and how they were addressed.
- How do you integrate the enforcement of access restrictions with other security and change management tools or protocols?
- Are there periodic reviews or assessments to validate the effective enforcement of access restrictions during system changes?
- How do you manage feedback or concerns related to access restrictions from stakeholders involved in system changes?
- How do you ensure that access restrictions during system changes do not inadvertently affect other critical operations or functionalities?
- How do you collaborate with external entities, industry groups, or security experts to enhance your access restriction protocols related to system changes?
- How do you ensure that the access restriction protocols for system changes align with the organization's broader cybersecurity objectives and NIST compliance requirements?



Configuration Management



CM.L2-3.4.8



Derived



Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

- Do you currently employ a blacklisting or whitelisting approach for software execution?
- How do you determine which software applications are placed on the whitelist or blacklist?
- What tools or solutions do you use to enforce these software execution policies?
- How frequently do you review and update the whitelist or blacklist?
- How do you handle exceptions or requests for software that is not on the approved list?
- How do you ensure users are aware of and adhere to the software execution policies in place?
- Are there alerts or mechanisms to detect and respond to attempts to run software not on the whitelist or on the blacklist?
- How do you manage updates or patches to software on the whitelist to ensure they remain compliant?
- How do you address potential vulnerabilities or threats associated with software on the whitelist?
- Describe any challenges or issues you've faced related to blacklisting or whitelisting and how they were addressed.
- How do you ensure third-party vendors or partners adhere to the organization's software execution policies?
- How do you verify the integrity and authenticity of software before adding it to the whitelist?
- How do you handle legacy software or applications in the context of blacklisting or whitelisting?
- How do you integrate the enforcement of these policies with other security tools or incident response systems?
- Are there periodic audits or assessments to validate the effectiveness of your software execution policies?
- How do you manage feedback or concerns from users or departments about software restrictions?
- How do you collaborate with external entities or industry peers to stay updated on software that should be blacklisted?
- Are there specific controls or restrictions for software execution on critical or sensitive systems?
- How do you ensure continuity in software access and execution during organizational changes, system upgrades, or the introduction of new technologies?
- How do you ensure that the blacklisting or whitelisting approach aligns with the organization's broader cybersecurity objectives and NIST compliance requirements?



Configuration Management



CM.L2-3.4.3



Derived



Track, review, approve or disapprove, and log changes to organizational systems.

- What tools or systems do you use to track changes made to organizational systems?
- Describe the process for reviewing proposed changes to the systems. Who is involved in this review?
- How do you ensure that all changes undergo a formal approval process before implementation?
- What criteria are used to approve or disapprove changes to the systems?
- How are disapproved changes communicated to relevant stakeholders, and how are they handled subsequently?
- How do you log changes, and what details are captured in these logs?
- How frequently are change logs reviewed, and by whom?
- How do you ensure that unauthorized changes are detected and addressed?
- Are there automated alerts or notifications set up for critical or high-impact changes?
- How do you handle emergency or urgent changes that might bypass the regular review process?
- How do you ensure that changes do not inadvertently introduce vulnerabilities or compromise security configurations?
- How do you manage dependencies and potential cascading effects of system changes?
- How do you ensure that third-party vendors or partners adhere to your organization's change management policies and procedures?
- How do you coordinate and communicate changes across departments or teams to minimize disruptions?
- How do you train and educate relevant personnel on the change management process and its importance?
- Describe any challenges or issues you've encountered in managing system changes, and how they were addressed.
- How do you integrate the change management process with other security tools, incident response systems, or risk management protocols?
- Are there periodic audits or assessments to validate the effectiveness of your change management process?
- How do you collect and address feedback or concerns related to the change management process?
- How do you ensure that the change management process aligns with the organization's broader cybersecurity objectives and NIST compliance requirements?



Configuration Management

CM.L2-3.4.2

Basic

Establish and enforce security configuration settings for information technology products employed in organizational systems.

- How do you determine the appropriate security configuration settings for various IT products in your organization?
- Describe the tools or platforms you use to enforce and monitor these security configuration settings.
- How do you ensure that all newly deployed or introduced IT products adhere to the defined security configurations?
- How frequently do you review and update the security configuration settings to reflect the evolving threat landscape and organizational needs?
- What processes are in place to test and validate the effectiveness of security configuration settings?
- How do you handle exceptions or custom configuration needs for specific systems or applications?
- Are there automated alerts or notifications set up to detect deviations from the defined security configurations?
- How do you educate and train relevant personnel about the importance of adhering to security configuration settings?
- How do you address non-compliance or deviations from the established security configurations?
- How do you manage updates, patches, or upgrades to IT products to ensure they don't compromise the defined security configurations?
- Describe any challenges or issues you've encountered related to security configuration management and how they were addressed.
- How do you ensure third-party vendors, partners, or integrated solutions adhere to your organization's security configuration standards?
- How do you incorporate feedback from security assessments, penetration tests, or vulnerability scans into refining your configuration settings?
- Are there periodic audits or assessments to validate the adherence to and effectiveness of security configurations?
- How do you handle legacy systems or applications in the context of security configuration management?
- How do you balance the need for system functionality and user convenience with the enforcement of security configurations?
- How do you ensure that security configurations do not inadvertently hamper critical business processes or functionalities?

- How do you collaborate with external entities, industry peers, or security experts to stay updated on best practices for security configurations?
- Are there specific controls or protocols for security configurations on critical, sensitive, or externally-facing systems?
- How do you ensure that the security configuration management process aligns with the organization's broader cybersecurity objectives and NIST compliance requirements?



Configuration Management



CM.L2-3.4.1



Basic



Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

- How do you establish baseline configurations for your organizational systems?
- Describe the tools or platforms used to maintain and manage inventories of hardware, software, firmware, and documentation.
- How frequently are these baseline configurations and inventories updated?
- How do you ensure that changes or updates to systems are reflected in the baseline configurations and inventories?
- What processes are in place to verify the accuracy and completeness of the system inventories?
- How do you track and manage system components throughout their development life cycles?
- How do you handle exceptions or deviations from the established baseline configurations?
- Are there automated alerts or mechanisms in place to detect unauthorized changes or additions to system components?
- How do you integrate configuration management with other security and change management processes?
- How do you ensure that third-party vendors or integrated solutions adhere to your organization's baseline configurations and are included in the inventories?
- How do you manage and track software licenses, versions, and patches in the system inventories?
- Describe any challenges or issues you've encountered related to baseline configuration and inventory management, and how they were addressed.
- How do you ensure that legacy systems or components are also included and managed within the baseline configurations and inventories?

- How do you handle decommissioning or retirement of system components in the context of baseline configurations and inventories?
- Are there periodic audits or assessments to validate the accuracy and adherence to baseline configurations and inventories?
- How do you ensure that the documented configurations and inventories are secure from unauthorized access or modification?
- How do you incorporate feedback from security assessments or vulnerability scans into refining your baseline configurations?
- How do you ensure continuity and accuracy in configuration and inventory management during organizational changes, system migrations, or the introduction of new technologies?
- How do you collaborate with external entities, industry peers, or security experts to stay updated on best practices for configuration and inventory management?
- How do you ensure that the baseline configuration and inventory management process aligns with the organization's broader cybersecurity objectives and NIST compliance requirements?



Configuration Management

CM.L2-3.4.4

Derived

Analyze the security impact of changes prior to implementation.

- How do you establish baseline configurations for your organizational systems?
- Describe the tools or platforms used to maintain and manage inventories of hardware, software, firmware, and documentation.
- How frequently are these baseline configurations and inventories updated?
- How do you ensure that changes or updates to systems are reflected in the baseline configurations and inventories?
- What processes are in place to verify the accuracy and completeness of the system inventories?
- How do you track and manage system components throughout their development life cycles?
- How do you handle exceptions or deviations from the established baseline configurations?
- Are there automated alerts or mechanisms in place to detect unauthorized changes or additions to system components?
- How do you integrate configuration management with other security and change management processes?
- How do you ensure that third-party vendors or integrated solutions adhere to your organization's baseline configurations and are included in the inventories?

- How do you manage and track software licenses, versions, and patches in the system inventories?
- Describe any challenges or issues you've encountered related to baseline configuration and inventory management, and how they were addressed.
- How do you ensure that legacy systems or components are also included and managed within the baseline configurations and inventories?

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

Preparing for Your CMMC Interview: Commonly Asked Questions – Identification and Authentication Edition

Identification and Authorization are the digital equivalents of checking someone's ID at the door. From a cybersecurity perspective, identification, and authentication work collaboratively to ensure that users are who they say they are before granting access to a system or network.

Key

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

Security Requirement Table of Contents

Identification and Authentication

- Obscure feedback of authentication information.....4
- Identify system users, processes acting on behalf of users, and devices.....5
- Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.....6
- Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.....7
- Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.....8
- Prevent reuse of identifiers for a defined period.....9
- Disable identifiers after a defined period of inactivity.....10
- Enforce a minimum password complexity and change of characters when new passwords are created.....11
- Prohibit password reuse for a specified number of generations.....12
- Allow temporary password use for system logons with an immediate change to a permanent password.....13
- Store and transmit only cryptographically-protected passwords.....15

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?



Identification and Authentication

3.5.11

Derived

Obscure feedback of authentication information

- How does your organization obscure feedback during user authentication processes?
- What mechanisms are in place to prevent the display of authentication details, such as passwords, in plain text?
- Do your authentication error messages avoid specifying the exact nature of the failure (e.g., not distinguishing between an incorrect username or password)?
- Are there any platforms or applications within your organization that don't adhere to the practice of obscuring authentication feedback? If so, how are they justified or managed?
- What measures have been implemented to prevent direct observation or "shoulder surfing" during authentication?
- How is obscured feedback handled in the context of multi-factor authentication?
- How do you ensure that third-party software or systems integrated into your environment also adhere to the practice of obscuring authentication feedback?
- What strategies are in place to ensure obscured feedback doesn't negatively impact user experience or lead to additional support issues?
- How do you handle feedback obscuration for authentication recovery or reset processes?
- How often do you review and update your methods for obscuring authentication feedback in light of evolving threats and best practices?
- Are there mechanisms in place to detect and alert on multiple failed authentication attempts?
- How do you educate users about the reasons and importance of obscured feedback during authentication?
- Are there specific challenges or considerations you've faced while implementing obscured feedback, and how were they addressed?
- How do you test or validate the effectiveness of obscured feedback mechanisms?
- How do you ensure that all updates or changes to authentication systems maintain the practice of obscuring feedback?
- Are there periodic security audits or assessments to verify the consistent application of obscured feedback across all systems?
- How do you handle exceptions or scenarios where authentication feedback might be less obscured?
- How do you stay updated on industry best practices or recommendations related to obscuring authentication feedback?

- In cases of user feedback or concerns related to obscured authentication feedback, how are they addressed?
- How do you ensure the organization's approach to obscuring authentication feedback aligns with NIST guidelines and broader cybersecurity objectives?



Identification and Authentication



IA.L1-3.5.1



Basic



Identify system users, processes acting on behalf of users, and devices.

- How does your organization identify and authenticate individual users accessing your systems?
- What mechanisms are in place to track and identify processes that act on behalf of authenticated users?
- How do you ensure unique identification of devices connecting to your systems?
- Describe the tools or platforms used to manage user and device identities.
- How do you handle shared accounts or group identities, if they exist?
- What measures are in place to prevent unauthorized users, processes, or devices from accessing the system?
- How frequently is the list of identified users, processes, and devices reviewed and updated?
- How do you manage and track third-party or external users accessing your systems?
- Describe the process for deprovisioning or removing users, processes, or devices that no longer require access.
- How do you ensure that processes acting on behalf of users don't exceed their authorized permissions?
- What authentication methods are used to verify the identity of users and devices?
- How do you handle exceptions or anomalies detected in the identification process?
- Are there automated alerts or mechanisms in place to detect and respond to unidentified or unauthorized users, processes, or devices?
- How do you integrate user, process, and device identification with other security systems or protocols?
- How do you manage user, process, and device identification in cloud environments or remote access scenarios?
- Describe any challenges or issues you've faced related to identifying users, processes, or devices and how they were addressed.
- How do you ensure that user, process, and device identification mechanisms are resilient against potential attacks or spoofing attempts?
- How do you stay updated on best practices and industry standards related to user, process, and device identification?

- Are there periodic security audits or assessments to validate the accuracy and effectiveness of your identification mechanisms?
- How do you ensure that the approach to identifying users, processes, and devices aligns with NIST guidelines and broader cybersecurity objectives?



Identification and Authentication

IA.L1-3.5.2

Basic

Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

- What authentication mechanisms are in place to verify user identities before granting system access?
- How do you verify the identity of processes acting on behalf of users?
- Describe the methods used to authenticate devices that seek to access organizational systems.
- Are multi-factor authentication (MFA) methods employed? If so, in what scenarios and how?
- How do you manage and securely store authentication credentials?
- How frequently are authentication policies and mechanisms reviewed and updated?
- Describe the process to handle authentication failures or repeated failed login attempts.
- How do you ensure that authentication methods are resilient against common attacks, such as phishing or brute force?
- What measures are in place to detect and respond to suspicious or anomalous authentication activities?
- How do you handle third-party or external entities' authentication to your systems?
- Are there any exceptions or scenarios where authentication might be bypassed or relaxed, and how are they justified and managed?
- Describe the tools or platforms used to manage and monitor authentication across organizational systems.
- How do you integrate authentication mechanisms with other security tools, such as intrusion detection systems or access control lists?
- How do you ensure the confidentiality and integrity of authentication data during transit and at rest?
- How do you manage the lifecycle of authentication credentials, including creation, rotation, and retirement?
- How do you educate and train users on the importance of secure authentication practices?
- Are there periodic security audits or assessments to validate the effectiveness of your authentication mechanisms?

- How do you stay updated on best practices and industry standards related to authentication?
- How do you handle user feedback or concerns related to authentication processes and procedures?
- How do you ensure that the approach to authenticating users, processes, and devices aligns with NIST guidelines and broader cybersecurity objectives?



Identification and Authentication



IA.L2-3.5.3



Derived



Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

- How is multifactor authentication implemented for privileged accounts within your organization?
- Describe the MFA mechanisms in place for network access to non-privileged accounts.
- What factors (e.g., something you know, something you have, something you are) are employed in your MFA setup?
- How do you ensure that MFA is consistently enforced for all privileged account access?
- Describe the process for onboarding users onto the MFA system.
- How do you handle situations where MFA might fail or be unavailable?
- Are there any exceptions to the MFA requirement, and if so, how are they justified and managed?
- How do you educate and train users on the importance of MFA and its usage?
- Describe the tools or platforms used to manage and enforce MFA.
- How do you integrate MFA with other security protocols or systems within the organization?
- How frequently do you review and update MFA settings, protocols, or mechanisms?
- How do you handle lost, stolen, or compromised MFA tokens or devices?
- Describe any challenges or issues you've faced related to implementing or maintaining MFA and how they were addressed.
- How do you ensure that third-party vendors or partners accessing your systems adhere to MFA requirements?
- How do you validate the effectiveness and security of your MFA mechanisms?
- Are there automated alerts or mechanisms to detect and respond to potential MFA breaches or bypass attempts?
- How do you manage MFA in remote work or mobile scenarios?
- How do you stay updated on best practices and industry standards related to multifactor authentication?

- Are there periodic security audits or assessments to verify consistent and effective implementation of MFA across all accounts?
- How do you ensure that the MFA implementation aligns with NIST guidelines and the broader cybersecurity objectives of your organization?



Identification and Authentication



IA.L2-3.5.4



Derived



Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

- What replay-resistant authentication mechanisms are currently employed by your organization?
- How do you differentiate between privileged and non-privileged accounts in terms of replay-resistant authentication?
- What tools or technologies are used to implement and enforce replay-resistant authentication?
- How do you handle instances where authentication tokens or credentials might be intercepted or captured?
- Are there automated alerts or mechanisms in place to detect and respond to potential replay attacks?
- How do you ensure that third-party software or integrated systems also employ replay-resistant authentication mechanisms?
- How frequently do you review and update your replay-resistant authentication methods in light of evolving threats and technologies?
- How do you test the effectiveness and resilience of your replay-resistant authentication mechanisms against potential attacks?
- Describe any challenges or issues you've faced related to implementing replay-resistant authentication and how they were addressed.
- Are there specific protocols or enhanced measures for replay-resistant authentication on critical systems or high-value targets?
- How do you handle legacy systems or applications in the context of replay-resistant authentication?
- How are users educated or trained about the importance and workings of replay-resistant authentication?
- How do you integrate replay-resistant authentication mechanisms with other security measures, such as multi-factor authentication?
- How do you manage and update cryptographic keys or secrets associated with replay-resistant mechanisms?

- Are there periodic security audits or assessments to validate the effectiveness and consistency of your replay-resistant authentication methods?
- How do you stay updated on industry best practices or recommendations related to replay-resistant authentication?
- In cases of user feedback or concerns related to authentication processes, how are they addressed?
- How do you ensure continuity of access during updates or changes to the replay-resistant authentication mechanisms?
- How do you manage backup or recovery scenarios while ensuring replay-resistant authentication is not compromised?
- How do you ensure that the approach to replay-resistant authentication aligns with NIST guidelines and broader cybersecurity objectives?



Identification and Authentication



IA.L2-3.5.5



Derived



Prevent reuse of identifiers for a defined period.

- How does your organization enforce policies to prevent the reuse of identifiers?
- What is the defined period during which identifiers cannot be reused?
- Describe the tools or systems in place that track and enforce this non-reuse period for identifiers.
- How do you handle situations where there's a need to reissue or reuse an identifier within the defined period?
- What mechanisms are in place to notify administrators or users about impending identifier expirations or renewals?
- How do you ensure that third-party systems or integrated platforms adhere to the non-reuse period for identifiers?
- Are there exceptions or scenarios where an identifier might be reused within the defined period, and how are they justified or managed?
- How do you educate and train relevant personnel about the importance of not reusing identifiers within the defined period?
- How do you handle historical data or logs containing old identifiers?
- Are there automated alerts or mechanisms in place to detect and respond to attempts to reuse identifiers within the defined period?
- How frequently is the non-reuse policy reviewed and potentially updated?

- How do you manage feedback or concerns related to the non-reuse period for identifiers?
- Describe any challenges or issues you've faced related to preventing identifier reuse and how they were addressed.
- How do you integrate the prevention of identifier reuse with other security and identity management protocols?
- Are there periodic security audits or assessments to validate the effective enforcement of the non-reuse period for identifiers?
- How do you ensure that archived or backup data also adheres to the non-reuse policy for identifiers?
- How do you stay updated on best practices and industry recommendations related to identifier management and non-reuse periods?
- How do you handle the decommissioning or revocation of identifiers, ensuring they aren't reused prematurely?
- Are there specific protocols or controls for preventing reuse of identifiers on critical or high-security systems?
- How do you ensure that the approach to preventing identifier reuse aligns with NIST guidelines and broader cybersecurity objectives?



Identification and Authentication



IA.L2-3.5.6



Derived



Disable identifiers after a defined period of inactivity.

- What is the defined period of inactivity after which an identifier is disabled in your systems?
- How do you monitor and track user activity to determine inactivity periods?
- What systems or tools are in place to automatically disable identifiers after the inactivity threshold is reached?
- How do you notify users when their identifiers have been disabled due to inactivity?
- What is the process for reactivating a disabled identifier?
- How do you ensure that the inactivity threshold balances security needs with user convenience?
- Are there exceptions or different inactivity thresholds for critical roles or accounts?
- How do you handle third-party or external user identifiers in terms of inactivity?
- Are there periodic reviews or audits to ensure that inactive identifiers are consistently disabled?
- How do you handle user feedback or concerns related to disabled identifiers due to inactivity?

- How do you educate users about the importance and rationale behind disabling identifiers after periods of inactivity?
- What measures are in place to detect any unauthorized attempts to access or reactivate disabled identifiers?
- How do you handle identifiers associated with automated processes or system accounts in terms of inactivity?
- Are there different inactivity thresholds for different types of systems or data sensitivity levels?
- How do you ensure that the disabling of identifiers does not inadvertently affect critical operations or functionalities?
- How do you document and maintain records of disabled identifiers?
- Are there any challenges or issues you've faced related to disabling identifiers due to inactivity, and how were they addressed?
- How do you integrate the process of disabling identifiers with other security protocols, such as logging or alerting mechanisms?
- How do you stay updated on best practices or industry standards related to identifier management and inactivity thresholds?
- How do you ensure that the approach to disabling identifiers after periods of inactivity aligns with NIST guidelines and broader cybersecurity objectives?



Identification and Authentication

IA.L2-3.5.7

Derived

Enforce a minimum password complexity and change of characters when new passwords are created.

- What are the specific criteria for password complexity currently enforced in your organization?
- How do you ensure that new passwords differ significantly from previously used passwords in terms of character changes?
- What systems or tools are in place to enforce and verify password complexity requirements?
- How do you handle exceptions or deviations from the established password complexity rules?
- How frequently are users prompted or required to change their passwords?
- How do you educate users about the importance of password complexity and the reasons behind the requirements?
- Are there automated alerts or notifications in place for users attempting to create non-compliant passwords?

- How do you ensure third-party systems or integrated platforms adhere to your organization's password complexity standards?
- How do you handle situations where legacy systems or applications don't support the desired password complexity requirements?
- Are there additional controls or restrictions for passwords related to high-privilege or critical accounts?
- How do you manage or monitor instances of users reusing old passwords or making minimal changes to meet the criteria?
- Are there periodic security audits or assessments to validate the enforcement of password complexity requirements?
- How do you incorporate feedback from security incidents, breaches, or attacks related to passwords into refining your complexity requirements?
- How do you ensure password complexity requirements don't inadvertently lead to negative user behaviors, such as writing down passwords?
- Do you use any additional mechanisms, like two-factor authentication, to supplement password complexity requirements?
- How do you stay updated on industry best practices or recommendations related to password complexity and management?
- How do you address user feedback or concerns related to password complexity requirements?
- Are there any challenges or issues you've faced related to enforcing password complexity, and how were they addressed?
- How do you integrate password complexity requirements with other security tools, protocols, or systems?
- How do you ensure that the approach to password complexity and character change aligns with NIST guidelines and broader cybersecurity objectives?



Identification and Authentication



IA.L2-3.5.8



Derived



Prohibit password reuse for a specified number of generations.

- How does your system enforce password history to prevent reuse?
- What is the specified number of generations for which password reuse is prohibited in your organization?
- Describe the tools or platforms you use to enforce this password policy.
- How do you handle exceptions or requests for password resets in light of this policy?

- Are users informed or educated about the prohibition on password reuse? How is this communicated?
- How frequently do users need to change their passwords in your organization?
- How do you ensure third-party applications or systems integrated into your environment adhere to the password reuse prohibition?
- Are there any systems or platforms within your organization that are exempt from this policy? If so, how are they managed?
- How do you handle scenarios where users attempt to reuse passwords from previous generations?
- Are there automated alerts or notifications in place to remind users about password changes without reusing old passwords?
- How do you store and secure password histories to ensure they aren't accessed or compromised?
- How do you balance the need for strong password policies with user convenience and usability?
- How does your password reuse policy integrate with other authentication and security measures, such as multi-factor authentication?
- Describe any challenges or issues you've faced related to enforcing password reuse prohibition and how they were addressed.
- How do you stay updated on best practices or recommendations related to password management and reuse?
- How do you handle user feedback or concerns related to the password reuse policy?
- Are there periodic security audits or assessments to verify adherence to the password reuse prohibition policy?
- How do you ensure that legacy systems or applications are compliant with the password reuse prohibition?
- Are there additional layers of security for privileged or administrative accounts concerning password reuse?
- How do you ensure that the approach to prohibiting password reuse aligns with NIST guidelines and your organization's broader cybersecurity objectives?



Identification and Authentication



IA.L2-3.5.9



Derived



Allow temporary password use for system logons with an immediate change to a permanent password.

- How does your organization handle temporary password issuance for system logons?
- What mechanisms are in place to ensure that users change temporary passwords upon their first logon?

- How do you ensure that temporary passwords are securely transmitted to users?
- What is the maximum lifespan of a temporary password if not used?
- Are there security measures in place to detect and prevent multiple failed login attempts with a temporary password?
- How do you manage and monitor the issuance and usage of temporary passwords?
- How do you ensure that the subsequent permanent passwords adhere to your organization's password complexity requirements?
- Describe any automated tools or platforms used to manage temporary password issuance and enforced change.
- How do you handle situations where a temporary password is not changed to a permanent one within the stipulated time?
- What is the process for revoking or invalidating a temporary password?
- How do you educate users about the security implications and proper usage of temporary passwords?
- Are there different protocols for temporary password issuance based on user roles or system sensitivity?
- How do you address scenarios where a temporary password might be intercepted or compromised?
- Describe any challenges or issues you've faced related to temporary password management and how they were addressed.
- Are there periodic security audits or assessments to validate the effectiveness and security of your temporary password protocols?
- How do you handle feedback or concerns from users or departments about temporary password issuance and management?
- How do you integrate temporary password management with other security tools or systems?
- How do you handle temporary password issuance for third-party vendors or external users?
- How do you stay updated on best practices and industry standards related to temporary password management?
- How do you ensure that your approach to managing temporary passwords aligns with NIST guidelines and your organization's broader cybersecurity objectives?



Identification and Authentication



IA.L2-3.5.10



Derived



Store and transmit only cryptographically-protected passwords.

- How does your organization ensure that passwords are stored in a cryptographically protected format?
- What cryptographic algorithms or methods do you employ for password protection?
- Describe the process and tools used to encrypt passwords before transmission.
- How do you manage and protect cryptographic keys associated with password encryption?
- Are there protocols in place to detect and alert on any attempts to transmit unprotected passwords?
- How frequently do you review and update cryptographic methods in light of evolving threats and best practices?
- How do you ensure that third-party tools or integrations also adhere to the practice of cryptographically protecting passwords?
- How do you handle password decryption at the receiving end, ensuring security during the process?
- Are there mechanisms in place to prevent unauthorized access or extraction of passwords, even in their encrypted form?
- How do you educate and train relevant personnel about the importance of password encryption and secure transmission?
- Describe any challenges or issues you've faced related to cryptographically protecting passwords and how they were addressed.
- How do you validate the effectiveness of cryptographic protections for stored and transmitted passwords?
- How do you manage and rotate cryptographic keys, ensuring their security and integrity?
- How do you handle legacy systems or platforms that might not fully support modern cryptographic methods?
- Are there periodic security audits or assessments to verify the consistent application of cryptographic protection for passwords?
- How do you handle situations where encrypted passwords need to be recovered or accessed for legitimate purposes?
- How do you ensure resilience against potential attacks aimed at decrypting protected passwords?
- How do you stay updated on industry best practices and recommendations related to password encryption and transmission?
- What procedures are in place for updating or evolving cryptographic methods if a vulnerability is found in the current method?

- How do you ensure that the approach to cryptographically protecting passwords 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.







40 Burton Hills Blvd
Suite 200
Nashville, TN 37215

info@redspin.com
www.redspin.com

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

Preparing for Your CMMC Interview: Commonly Asked Questions – Maintenance Edition

This domain focuses on the health and servicing of our critical systems, much like a routine health check-up or scheduled car service. It requires consistent upkeep, servicing, and updating of an organization's systems, hardware, and software to ensure optimal functionality. This regular maintenance can help to detect and resolve minor issues before they escalate, and is performed through periodic assessment and updating of systems, such as patching vulnerabilities, such that the organization may guard against exploitation of known or emerging vulnerabilities.

Key

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

Security Requirement Table of Contents

Maintenance

- Perform maintenance on organizational systems.....4
- Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.....5
- Ensure equipment removed for off-site maintenance is sanitized of any CUI.....6
- Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.....7
- Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.....8
- Supervise the maintenance activities of maintenance personnel without required access authorization.....9

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?



Maintenance

MA.L2-3.7.1

Basic

Perform maintenance on organizational systems.

- How frequently do you perform system maintenance?
- Describe the process for scheduling and announcing planned maintenance activities.
- What tools or platforms do you use for system maintenance?
- How do you ensure that maintenance activities do not inadvertently introduce vulnerabilities?
- How do you manage and track third-party vendors or contractors involved in system maintenance?
- Are there specific protocols or procedures for maintenance on critical or high-security systems?
- How do you handle unscheduled or emergency maintenance requirements?
- How do you test systems post-maintenance to ensure their functionality and security?
- What documentation or logging is generated for each maintenance activity, and how is it stored?
- How do you manage system backups or data integrity during maintenance activities?
- What training or certification do maintenance personnel undergo to ensure they adhere to security standards?
- How do you integrate system maintenance with other security protocols, like vulnerability management or incident response?
- Describe any challenges or issues you've faced during system maintenance and how they were addressed.
- How do you notify stakeholders or users about maintenance activities, especially if there might be system downtime?
- How do you ensure that third-party software or tools used during maintenance are secure and compliant with organizational standards?
- Are there automated mechanisms in place to monitor and report on system health and potential maintenance needs?
- How do you validate the success and effectiveness of maintenance activities?
- How do you review and refine maintenance protocols based on feedback or post-maintenance assessments?
- Are there periodic security audits or assessments specifically targeting maintenance activities and their impact on system security?
- How do you ensure that the approach to system maintenance aligns with NIST guidelines and broader cybersecurity objectives?



Maintenance

MA.L2-3.7.2

Basic

Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

- What controls are in place to ensure only authorized tools are used for system maintenance?
- How do you vet and approve techniques or mechanisms employed during system maintenance?
- Describe the authentication and authorization processes in place for personnel conducting system maintenance.
- How do you ensure that third-party maintenance tools adhere to your organization's security controls?
- What logging or auditing capabilities are in place to track system maintenance activities?
- How do you control and monitor remote system maintenance activities?
- Are there specific protocols or controls for maintenance activities on critical or sensitive systems?
- How do you ensure the timely patching or updating of maintenance tools to address known vulnerabilities?
- Describe any encryption or security measures employed during data transfer for maintenance activities.
- How do you handle the storage and disposal of data or logs generated during system maintenance?
- How do you train and educate maintenance personnel on security best practices and protocols?
- Are there periodic security assessments or audits to validate the controls on system maintenance tools and techniques?
- How do you handle exceptions or emergency maintenance requirements in terms of security controls?
- How do you ensure that maintenance activities do not inadvertently introduce new vulnerabilities or risks?
- What controls are in place to restrict or monitor the installation of third-party or unauthorized software during maintenance?
- How do you manage feedback or concerns related to system maintenance from other departments or stakeholders?
- How do you stay updated on industry best practices or recommendations related to secure system maintenance?
- Describe any challenges or issues you've faced related to controlling system maintenance activities and how they were addressed.
- How do you ensure that third-party vendors or partners adhere to your organization's maintenance control standards?

- How do you ensure that the approach to controlling system maintenance activities aligns with NIST guidelines and broader cybersecurity objectives?



Maintenance



MA.L2-3.7.3



Derived



Ensure equipment removed for off-site maintenance is sanitized of any CUI.

- How do you identify equipment that contains or has accessed CUI before it's sent off-site for maintenance?
- Describe the process used to sanitize equipment of CUI prior to off-site maintenance.
- What tools or software are used to ensure complete sanitization of CUI from the equipment?
- How do you verify or validate that the sanitization process has been effective in removing all traces of CUI?
- What protocols are in place for handling equipment that cannot be adequately sanitized before off-site maintenance?
- How do you maintain a chain of custody or track equipment that is sent off-site for maintenance?
- Are there specific agreements or contracts with maintenance vendors regarding the handling and protection of CUI?
- How do you handle the potential backup or retention of CUI during the sanitization process?
- Describe any training or awareness programs in place for personnel responsible for sanitizing equipment of CUI.
- How do you address situations where equipment containing CUI is sent off-site for emergency maintenance or repairs?
- Are there automated tools or alerts in place to detect CUI on equipment designated for off-site maintenance?
- How do you handle potential data remnants or hidden storage areas on equipment that might contain CUI?
- Describe any challenges or issues you've faced related to sanitizing equipment of CUI and how they were addressed.
- How do you ensure the recovery or restoration of non-CUI data on equipment after the sanitization process?
- Are there periodic audits or assessments to verify the effectiveness of CUI sanitization procedures for off-site maintenance?

- How do you handle feedback or concerns related to the sanitization of equipment containing CUI?
- How do you collaborate with external entities, industry peers, or security experts to enhance your sanitization practices for CUI?
- Are there specific protocols or considerations for different types of equipment, such as servers, workstations, mobile devices, or storage devices?
- How do you ensure that the sanitization process adheres to NIST guidelines and other relevant standards?
- How do you document and maintain records of sanitization processes and verifications for equipment sent off-site?



Maintenance

MA.L2-3.7.4

Derived

Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

- What procedures are in place to check media with diagnostic and test programs for malicious code?
- How do you ensure that all media, regardless of its source, undergoes this checking process before use?
- Describe the tools or software you use for scanning and detecting malicious code on such media.
- How frequently are these scanning tools or software updated to detect the latest threats?
- How do you handle media that is found to contain malicious code?
- What protocols are in place for reporting and addressing incidents related to malicious code detection?
- How do you ensure that third-party or externally sourced diagnostic/test media is checked for malicious code before use?
- Are there any exceptions or scenarios where media might bypass this checking process? If so, how are they justified or managed?
- How do you train and educate relevant personnel about the importance of checking media for malicious code?
- Are there automated alerts or mechanisms in place to detect unauthorized or unchecked media usage within organizational systems?
- How do you verify the integrity and authenticity of diagnostic and test programs on the media?
- Describe any challenges or issues you've faced related to checking media for malicious code and how they were addressed.
- How do you ensure that the checking process doesn't inadvertently affect the functionality of legitimate diagnostic and test programs?

- How do you handle media that is reused or repurposed for diagnostic and test purposes?
- How do you collaborate with external entities, industry peers, or security experts to stay updated on best practices for media checking?
- Are there periodic security audits or assessments to verify the consistent application of malicious code checking on all media?
- How do you manage feedback or concerns related to the media checking process?
- How do you balance the need for rapid diagnostics or testing with the time required for thorough malicious code checks?
- How do you stay updated on emerging threats or attack vectors that might bypass traditional media checking mechanisms?
- How do you ensure that the approach to checking media for malicious code aligns with NIST guidelines and broader cybersecurity objectives?



Maintenance

MA.L2-3.7.5

Derived

Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

- How does your organization implement multifactor authentication for nonlocal maintenance sessions?
- What factors or methods are used as part of your MFA process for nonlocal maintenance?
- Describe the tools or platforms used to enforce MFA for these sessions.
- How do you ensure that nonlocal maintenance sessions are terminated upon completion?
- Are there any automated mechanisms in place to detect and terminate inactive nonlocal maintenance sessions?
- How do you handle exceptions or scenarios where MFA might be bypassed or not possible?
- How do you train and educate relevant personnel about the importance of MFA for nonlocal maintenance sessions?
- What measures are in place to protect against potential MFA bypass or spoofing attempts?
- How do you verify the identity and authenticity of external entities initiating nonlocal maintenance sessions?
- How do you log and monitor nonlocal maintenance sessions, especially those requiring MFA?
- Describe any challenges or issues you've encountered related to MFA for nonlocal maintenance and how they were addressed.

- How do you integrate MFA enforcement with other security systems or protocols?
- How frequently do you review and update your MFA mechanisms and policies for nonlocal maintenance sessions?
- Are there specific controls or protocols for MFA in critical or high-security systems during nonlocal maintenance?
- How do you handle feedback or concerns from users or technicians related to MFA during nonlocal maintenance?
- How do you ensure continuity in maintenance operations while enforcing MFA and session termination protocols?
- How do you collaborate with external entities, industry peers, or security experts to stay updated on best practices for MFA during nonlocal maintenance?
- Are there periodic security audits or assessments to verify the consistent application of MFA and session termination for nonlocal maintenance?
- How do you ensure that third-party vendors or partners adhere to your organization's MFA requirements for nonlocal maintenance?
- How do you ensure that the approach to MFA and session termination for nonlocal maintenance aligns with NIST guidelines and broader cybersecurity objectives?



Maintenance

MA.L2-3.7.6

Derived

Supervise the maintenance activities of maintenance personnel without required access authorization.

- How do you identify and track maintenance personnel who do not have the required access authorization?
- What protocols are in place to ensure that such maintenance personnel are always supervised during their activities?
- Who within the organization is responsible for supervising these maintenance activities?
- Describe the process or measures to ensure unauthorized personnel do not access sensitive or classified information during maintenance.
- How do you handle situations where maintenance needs to be performed urgently or outside of regular business hours?
- What training or guidelines are provided to supervisors overseeing maintenance personnel without required access authorization?
- How do you log and document the activities of maintenance personnel who are supervised?

- Are there any tools or technologies in place to aid in the supervision of maintenance activities, such as video surveillance or real-time monitoring?
- How do you handle scenarios where maintenance personnel without the required access authorization need to interact with third-party vendors or external systems?
- What measures are in place to prevent or detect unauthorized actions or deviations by maintenance personnel during their activities?
- How do you ensure that the maintenance performed by such personnel does not inadvertently introduce vulnerabilities or security risks?
- Are there periodic audits or reviews of the supervision process to ensure its effectiveness and adherence to protocols?
- Describe any challenges or issues you've encountered related to supervising maintenance personnel without required access, and how they were addressed.
- How do you handle feedback or concerns from supervisors or other staff related to this supervision process?
- How do you stay updated on best practices and industry standards related to supervising maintenance activities?
- How do you manage scenarios where maintenance personnel require temporary access to areas or data beyond their usual scope?
- How do you ensure that third-party maintenance providers or vendors adhere to your supervision protocols?
- How do you validate the credentials or background of maintenance personnel before they perform their tasks?
- Are there specific protocols for supervising maintenance activities in critical or high-security environments?
- How do you ensure that the approach to supervising maintenance personnel aligns with NIST guidelines and your organization's 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

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.

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.







40 Burton Hills Blvd
Suite 200
Nashville, TN 37215

info@redspin.com
www.redspin.com

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

This domain emphasizes a thorough review and vetting of all personnel to ensure these individuals can be trusted with access to sensitive information. This is typically performed through an initial background check, ongoing review of accesses, and regular training; it is intended to mitigate the risks associated with our ‘human firewalls’.

Key

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

Security Requirement Table of Contents

Personnel Security

- Screen individuals prior to authorizing access to organizational systems containing CUI.....4
- Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.....5

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?



Personnel Security

PS.L2-3.9.1

Basic

Screen individuals prior to authorizing access to organizational systems containing CUI.

- What is your process for screening individuals before granting them access to systems with CUI?
- What specific criteria or checks are included in the screening process?
- How do you verify the provided information of individuals during the screening process?
- Are there different levels of screening based on the sensitivity or classification of the CUI?
- How do you ensure that the screening process complies with legal and privacy regulations?
- What mechanisms are in place to re-screen individuals at periodic intervals or upon role changes?
- How do you manage and document the results of individual screenings?
- What is the procedure for denying access based on the results of a screening?
- How do you handle third-party or external contractors in the screening process?
- Are individuals made aware of the reasons for screening and the criteria being checked?
- How do you ensure that the screening process is consistently applied across all departments and teams?
- How do you address potential false positives or disputes arising from the screening process?
- Describe any challenges or issues you've faced related to screening individuals and how they were addressed.
- How do you train or educate relevant personnel about the importance and procedures of the screening process?
- How do you integrate the screening process with other security measures, such as access controls or user authentication?
- Are there periodic audits or assessments to validate the effectiveness and consistency of your screening process?
- How do you stay updated on best practices or legal requirements related to screening individuals for access to CUI?
- How do you handle the screening process in emergency or urgent situations requiring rapid access to CUI?
- How do you ensure that the screening process doesn't inadvertently hamper operational efficiency or critical business functions?
- How do you ensure that the approach to screening individuals prior to granting access to CUI aligns with NIST guidelines and broader cybersecurity objectives?



Personnel Security

PS.L2-3.9.2

Basic

Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers

- How does your organization handle access to systems containing CUI during personnel terminations?
- What processes are in place to ensure that access rights to CUI are revoked or modified during personnel transfers?
- Describe the timeline and immediacy of actions taken to protect CUI when an employee is terminated.
- How do you ensure that transferred employees do not retain unauthorized access to CUI from their previous roles?
- Are there automated systems or alerts in place to notify IT or security teams of personnel terminations or transfers?
- How do you handle the physical and digital assets (like devices or media) that might contain CUI when an employee is terminated or transferred?
- What measures are in place to ensure that former employees cannot access organizational systems containing CUI remotely?
- How do you audit or verify the successful removal or modification of access rights after personnel actions?
- Describe any challenges or issues you've faced in protecting CUI during personnel actions and how they were addressed.
- How do you handle situations where a terminated employee had unique knowledge or control over systems containing CUI?
- What training or awareness programs are in place to educate HR and management about the importance of timely notifications related to personnel actions?
- How do you ensure third-party vendors or partners protect CUI during their own personnel actions?
- Are there periodic security reviews or assessments to validate the protection of CUI during and after personnel actions?
- How do you address potential insider threats related to personnel terminations or transfers concerning CUI?
- How do you manage backup or archived data containing CUI related to terminated or transferred personnel?
- How do you ensure the timely return or secure disposal of physical documents containing CUI from terminated or transferred employees?

- How do you handle shared or group accounts in the context of personnel actions, especially if they have access to CUI?
- What incident response measures are in place if unauthorized access to CUI is detected after a personnel action?
- How do you collaborate with other departments, like HR, to streamline and ensure the protection of CUI during personnel actions?
- How do you ensure that the approach to protecting CUI during and after personnel actions aligns with NIST guidelines and the broader cybersecurity objectives of the organization?

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

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

Picture a bank with security guards and a vault, or a castle with a moat and drawbridge. These physical barriers ensure that the actual systems, devices, and storage locations for sensitive information are physically secure. The focus is on implementing tangible measures to prevent unauthorized physical access to facilities, equipment, and other resources as well as, protecting against environmental hazards. This may be implemented through a variety of protective measures, including security guards, visitor control desks, CCTV cameras, badge readers, secured server/storage rooms, and more.

Key

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

Security Requirement Table of Contents

Physical Protection

- Enforce safeguarding measures for CUI at alternate work sites.....4
- Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.....5
- Protect and monitor the physical facility and support infrastructure for organizational systems.....6
- Escort visitors and monitor visitor activity.....7
- Maintain audit logs of physical access.....8
- Control and manage physical access devices.....9

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?



Physical Protection

PE.L2-3.10.6

Derived

Enforce safeguarding measures for CUI at alternate work sites.

- How does your organization define and identify alternate work sites?
- What specific safeguarding measures are implemented for CUI when accessed or processed at alternate work sites?
- How do you ensure employees are aware of and adhere to CUI safeguarding measures when working remotely or off-site?
- Are there specific tools or technologies in place to secure CUI when accessed from alternate locations?
- How do you monitor and log access to CUI from off-site locations?
- How do you handle the secure transmission of CUI between primary and alternate work sites?
- What measures are in place to prevent unauthorized access or disclosure of CUI at alternate work sites?
- How do you ensure the physical security of devices or materials containing CUI at off-site locations?
- Are there specific training programs or guidelines provided to employees about managing CUI at alternate work sites?
- How do you manage and secure CUI on portable devices such as laptops or USB drives?
- What incident response measures are in place for potential breaches or unauthorized access to CUI at alternate sites?
- How frequently do you review and update policies related to safeguarding CUI at off-site locations?
- How do you handle situations where third-party vendors or partners access CUI from alternate work sites?
- Are there periodic security audits or checks for devices or locations involved in off-site CUI processing?
- How do you ensure encrypted storage and transmission of CUI when accessed from remote or alternate sites?
- How do you verify the security posture of alternate work sites, especially if they are personal or home environments?
- How do you manage feedback or concerns from employees regarding the safeguarding of CUI at off-site locations?
- Are there specific controls or restrictions on the types of CUI that can be accessed or processed at alternate work sites?
- How do you collaborate with other entities or industry peers to stay updated on best practices for safeguarding CUI at off-site locations?
- How do you ensure that your approach to safeguarding CUI at alternate work sites aligns with NIST guidelines and broader cybersecurity objectives?



Physical Protection

PE.L1-3.10.1

Basic

Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

- How do you control physical access to your organizational systems and equipment?
- What authentication mechanisms (e.g., access cards, biometrics) are in place to ensure only authorized individuals gain physical access?
- Describe the process for authorizing individuals to have physical access to specific areas or equipment.
- How do you track and log physical access to sensitive areas where systems and equipment are housed?
- How frequently is the list of individuals with authorized physical access reviewed and updated?
- Are there security personnel or surveillance systems in place to monitor and enforce physical access controls?
- How do you handle visitors or third-party contractors who require temporary physical access?
- Describe the protocols in place for quickly revoking physical access when an individual's authorization is terminated or changed.
- How do you ensure that physical access controls are maintained during emergencies or special circumstances?
- What measures are in place to detect and respond to unauthorized physical access attempts?
- How do you integrate physical access controls with other security systems or protocols, such as intrusion detection systems?
- How do you handle physical access controls in remote or secondary facilities, if applicable?
- Describe any challenges or incidents related to unauthorized physical access and how they were addressed.
- How do you educate and train relevant personnel about the importance of and procedures for physical access controls?
- Are there periodic security drills or simulations to test the effectiveness of physical access controls?
- How do you stay updated on best practices and industry standards related to physical access control?
- Are backup or redundant power supplies in place to ensure access control mechanisms remain operational during power outages?
- Are there periodic security audits or assessments to validate the adherence to and effectiveness of physical access controls?
- How do you ensure that physical security measures don't inadvertently hamper legitimate business operations or emergency responses?

- How do you ensure that the approach to controlling physical access aligns with NIST guidelines and broader cybersecurity objectives?



Physical Protection



PE.L2-3.10.2



Basic



Protect and monitor the physical facility and support infrastructure for organizational systems.

- How do you ensure the physical security of facilities housing your organizational systems?
- What access control measures are in place for these facilities?
- Describe the surveillance or monitoring systems deployed at these facilities.
- How do you manage and track authorized personnel access to these facilities?
- What measures are in place to detect and respond to unauthorized access or breaches in the physical facility?
- How do you protect the supporting infrastructure, such as power supplies, cooling systems, and network connections?
- Are there automated alerts or systems in place to notify of any disruptions or issues in the support infrastructure?
- How frequently do you review and test the physical security measures in place?
- Describe any backup or redundancy systems in place for critical infrastructure components.
- How do you handle third-party or vendor access to the physical facilities?
- What training or awareness programs are in place to ensure staff understand and adhere to physical security protocols?
- How do you integrate physical security with other security and incident response systems?
- Describe any challenges or issues you've encountered related to physical facility security and how they were addressed.
- How do you ensure continuous monitoring and protection of facilities in the event of emergencies or natural disasters?
- Are there periodic drills or exercises to test the effectiveness and readiness of physical security measures?
- How do you handle the disposal or decommissioning of equipment to ensure data security within the facility?
- How do you manage and secure remote or secondary facilities, if applicable?

- How do you stay updated on best practices and industry standards related to physical security and infrastructure protection?
- Are there periodic security audits or assessments to validate the effectiveness of your physical facility protection measures?
- How do you ensure that the approach to protecting and monitoring physical facilities and infrastructure aligns with NIST guidelines and broader cybersecurity objectives?



Physical Protection



PE.L1-3.10.3



Derived



Escort visitors and monitor visitor activity.

- How does your organization manage and control physical access for visitors?
- What procedures are in place to ensure visitors are escorted at all times while in secure or sensitive areas?
- How do you verify the identity of visitors before granting them access?
- What training or guidelines are provided to staff responsible for escorting visitors?
- Describe the mechanisms or tools used to monitor visitor activity during their stay.
- How are visitors made aware of the organization's security policies and their responsibilities while on-site?
- How do you handle visitors who need access to sensitive or restricted areas?
- Are there specific protocols or requirements for visitors from foreign entities or third-party vendors?
- How do you ensure that visitors don't inadvertently access or view sensitive information or systems?
- What processes are in place for logging visitor entries, exits, and their activities during the visit?
- How frequently are visitor logs reviewed, and by whom?
- Are there automated systems or surveillance tools in place to assist with monitoring visitor activity?
- How do you manage and respond to any security incidents or policy violations involving visitors?
- Describe any challenges or issues you've encountered related to escorting or monitoring visitors and how they were addressed.
- Are there periodic drills or assessments to test the effectiveness of your visitor management protocols?
- How do you ensure that visitor management procedures don't interfere with business operations or events?

- How do you handle scenarios where visitors require repeated or prolonged access, such as contractors or consultants?
- Are there specific protocols for managing visitor access during emergencies or special events?
- How do you gather feedback or concerns from staff and visitors related to the visitor management process?
- How do you ensure that your approach to escorting and monitoring visitors aligns with NIST guidelines and broader security objectives?



Physical Protection

PE.L1-3.10.4

Derived

Maintain audit logs of physical access.

- How does your organization log physical access events to your facilities or secure areas?
- What tools or systems are used to capture and store these physical access logs?
- How long are physical access logs retained, and where are they stored?
- What specific details or data points are captured in the physical access logs?
- How frequently are the physical access logs reviewed, and by whom?
- Are there automated alerts set up for unauthorized or suspicious physical access attempts?
- How do you ensure the integrity and confidentiality of the physical access logs?
- Describe the process for granting and revoking physical access permissions to different areas of your facility.
- How do you handle physical access logging for temporary or guest visitors?
- What measures are in place to ensure that physical access logs are complete and not tampered with?
- How are physical access logs integrated with other security systems or incident response protocols?
- How do you manage and audit third-party or vendor physical access to your facilities?
- Describe any challenges or issues you've encountered related to physical access logging and how they were addressed.
- How do you ensure that physical access logs are compliant with data protection or privacy regulations?
- Are there periodic security audits or assessments to validate the comprehensiveness and accuracy of your physical access logs?
- How do you handle the disposal or archiving of older physical access logs?

- How do you train security personnel or staff responsible for managing and reviewing physical access logs?
- How do you address discrepancies or anomalies detected in the physical access logs?
- How do you stay updated on best practices and industry standards related to physical access logging?
- How do you ensure that the approach to maintaining physical access audit logs aligns with NIST guidelines and broader cybersecurity objectives?



Physical Protection



:E.L1-3.10.5



Derived



Control and manage physical access devices.

- What types of physical access devices does your organization use (e.g., key cards, biometric scanners, RFID tags)?
- How do you ensure the security and integrity of these physical access devices?
- Describe the process for issuing, activating, and deactivating physical access devices.
- How do you track and monitor the use of physical access devices across your facilities?
- What measures are in place to prevent cloning, tampering, or unauthorized use of physical access devices?
- How frequently do you audit the usage logs of physical access devices?
- How do you handle lost, stolen, or compromised physical access devices?
- Are there automated alerts or mechanisms to detect suspicious or anomalous activity related to physical access devices?
- How do you integrate physical access device controls with other security systems, such as surveillance cameras or intrusion detection systems?
- Describe the process for updating or upgrading the technology or security features of physical access devices.
- How do you manage and control visitor or temporary physical access devices?
- What training or awareness programs are in place for employees regarding the proper use and security of physical access devices?
- How do you ensure redundancy or backup access mechanisms in case of failure or malfunction of primary physical access devices?
- Describe any challenges or issues you've faced related to managing physical access devices and how they were addressed.

- Are there specific protocols for the use of physical access devices in high-security areas or sensitive locations within your facilities?
- How do you handle the decommissioning or disposal of outdated or unused physical access devices?
- How do you verify the authenticity and security of third-party or externally sourced physical access devices?
- How do you stay updated on industry best practices and emerging threats related to physical access devices?
- Are there periodic security reviews or tests to validate the effectiveness and security of your physical access devices?
- How do you ensure that the management and control of physical access devices align with NIST guidelines and your organization's 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.



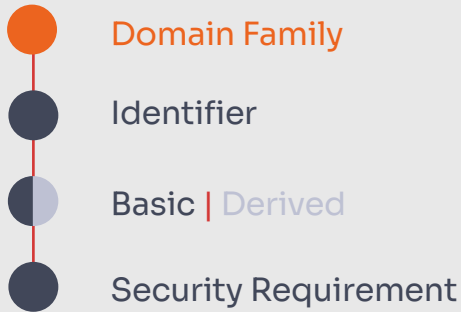
40 Burton Hills Blvd
Suite 200
Nashville, TN 37215

info@redspin.com
www.redspin.com

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.

Key



Security Requirement Table of Contents

Risk Assessment

- Remediate vulnerabilities in accordance with risk assessments.....4
- 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 CU.....5
- Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.....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?



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?



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?

- 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?

- 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?

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

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.

Key

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

Security Requirement Table of Contents

Security Assessment

- Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.....4
- Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.....5
- Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.....6
- 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.....7

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?



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?

- 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?

- 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?

- 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?

- 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?

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

Preparing for Your CMMC Interview: Commonly Asked Questions – System and Communications Protection Edition

This domain emphasizes the safeguarding of information as it is transmitted across networks and systems, ultimately ensuring that messages and/or data sent and received can remain confidential and unaltered. This may include measures such as encryption, firewalls, intrusion detection systems (IDSs), secure communication protocols, and more, ultimately securing this data from external threats.

Key

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

Security Requirement Table of Contents

System and Communications Protection

- Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).....5
- Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.....6
- Control and monitor the use of mobile code.....7
- Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.[29].8
- Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.....9
- Establish and manage cryptographic keys for cryptography employed in organizational systems.....10
- Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.....11
- Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).....12
- Protect the authenticity of communications sessions.....14
- Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.....15
- Prevent unauthorized and unintended information transfer via shared system resources.....16
- Separate user functionality from system management functionality.....17
- Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.....19
- Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.....20
- Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.....21
- Protect the confidentiality of CUI at rest.....22

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 Communications Protection

SC.L2-3.13.7

Derived

Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

- How does your organization address the risk of split tunneling in its remote access policies?
- What mechanisms or tools are in place to detect and prevent remote devices from establishing split tunnels?
- How do you ensure that remote devices connected to your organizational systems don't simultaneously communicate with external networks?
- What monitoring solutions are employed to oversee remote device connections and ensure compliance with the no-split-tunneling policy?
- Are users educated or trained about the risks and prohibitions associated with split tunneling?
- How do you handle violations or attempts to bypass the split tunneling prevention mechanisms?
- How do you manage exceptions or scenarios where split tunneling might be required for specific business purposes?
- Describe any challenges or issues you've faced related to preventing split tunneling and how they were addressed.
- How do you ensure third-party or partner devices connecting to your systems adhere to the no-split-tunneling policy?
- Are there automated alerts or notifications set up to detect potential split tunneling activities?
- How do you test or validate the effectiveness of mechanisms in place to prevent split tunneling?
- How do you handle software or applications on remote devices that might inherently use split tunneling features?
- What processes are in place to review and update the split tunneling prevention mechanisms in light of evolving threats or technologies?
- Are there periodic security audits or assessments to validate adherence to the no-split-tunneling policy and its effectiveness?
- How do you manage user feedback or concerns related to the restriction of split tunneling?
- How do you ensure continuity of operations and user experience while enforcing the no-split-tunneling policy?
- How do you integrate split tunneling prevention with other security measures or VPN configurations?

- How do you stay informed about industry best practices or emerging threats related to split tunneling?
- In scenarios of remote global access, how do you handle split tunneling considerations given varying network conditions or requirements?
- How do you ensure that the approach to preventing split tunneling aligns with NIST guidelines and the organization's broader cybersecurity objectives?



System and Communications Protection



SC.L2-3.13.14



Derived



Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

- How does your organization implement security controls for VoIP technologies?
- What tools or platforms are used to monitor VoIP traffic and usage within your environment?
- How do you ensure encryption and secure protocols are in place for VoIP communications?
- Are there specific policies or guidelines provided to employees regarding the secure use of VoIP technologies?
- How do you handle authentication and access control for VoIP systems and endpoints?
- What measures are in place to detect and prevent unauthorized or malicious VoIP traffic?
- How do you segregate or isolate VoIP traffic from other network traffic to ensure its security?
- How frequently are VoIP security configurations and controls reviewed and updated?
- How do you manage and secure VoIP endpoints, such as phones, softphones, or VoIP applications?
- Are there automated alerts or mechanisms in place to detect anomalies or potential security incidents related to VoIP?
- Describe any challenges or issues you've faced related to VoIP security and how they were addressed.
- How do you ensure third-party VoIP solutions or services used by your organization adhere to security best practices?
- How do you handle data retention, backup, and recovery for VoIP systems and communications?
- How do you educate and train users about potential risks and best practices related to VoIP usage?
- How do you manage patches, updates, or vulnerabilities associated with VoIP software or hardware?
- How do you ensure continuity and availability of VoIP services while maintaining security?
- Are there specific protocols or controls for VoIP communications that involve sensitive or confidential information?

- How do you integrate VoIP security monitoring with other security tools or incident response systems?
- Are there periodic security audits or assessments specific to VoIP technologies and their usage?
- How do you ensure that the approach to controlling and monitoring VoIP aligns with NIST guidelines and broader cybersecurity objectives?



System and Communications Protection



SC.L2-3.13.13



Derived



Control and monitor the use of mobile code.

- How does your organization define mobile code in the context of its systems and operations?
- What policies and procedures are in place for the use of mobile code?
- How do you ensure that only authorized mobile code runs on organizational systems?
- Describe the tools or mechanisms used to monitor the execution of mobile code.
- How do you verify the authenticity and integrity of mobile code before it's executed?
- Are there specific repositories or sources from which mobile code is approved or allowed?
- How do you handle exceptions or requests to use mobile code that falls outside of established policies?
- How do you educate users about the risks and policies associated with mobile code?
- Are there automated alerts or mechanisms in place to detect unauthorized mobile code execution?
- How do you integrate mobile code monitoring with other security systems or protocols?
- What measures are in place to prevent or mitigate mobile code from exploiting vulnerabilities in organizational systems?
- How frequently is the list of authorized mobile code sources or repositories reviewed and updated?
- Describe any challenges or issues you've encountered related to mobile code and how they were addressed.
- How do you handle updates or patches to mobile code to ensure they don't introduce security risks?
- How do you ensure third-party vendors or integrated solutions adhere to your organization's mobile code policies?
- How do you manage mobile code in cloud environments or remote access scenarios?
- Are there specific controls or restrictions for mobile code on critical or high-security systems?
- How do you stay updated on best practices and industry standards related to mobile code security?

- Are there periodic security audits or assessments to validate the control and monitoring of mobile code?
- How do you ensure that the approach to controlling and monitoring mobile code aligns with NIST guidelines and broader cybersecurity objectives?



System and Communications Protection

SC.L2-3.13.12

Derived

Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.[29].

- How do you ensure that collaborative computing devices cannot be remotely activated without proper authorization?
- What mechanisms or features are in place to provide clear indications to users when collaborative computing devices are in use?
- How do you handle exceptions or approved scenarios where remote activation is necessary?
- Describe the tools or platforms used to monitor and manage remote access to collaborative computing devices.
- Are there automated alerts or mechanisms in place to detect unauthorized remote activation attempts?
- How do you educate users about the indications of device usage and the risks associated with unauthorized remote activation?
- What measures are in place to protect against potential attacks or unauthorized access to collaborative computing devices?
- How frequently are the configurations and settings related to this practice reviewed and updated?
- How do you handle third-party or external devices that might be integrated into your collaborative computing environment?
- How do you ensure that software or firmware updates to collaborative computing devices don't inadvertently alter the security settings related to remote activation?
- Describe any challenges or issues you've faced related to remote activation of devices and how they were addressed.
- How do you test or validate the effectiveness of mechanisms that indicate device usage to users present at the device?
- How do you manage and track user feedback or concerns related to this practice?
- Are there specific protocols or measures in place for high-security environments or sensitive meetings?
- How do you integrate this practice with other security protocols, especially those related to remote access or device management?

- How do you handle older or legacy collaborative computing devices in the context of this practice?
- Are there periodic security audits or assessments to validate the effective enforcement of this practice?
- How do you stay updated on industry best practices or threats related to remote activation of collaborative computing devices?
- In the event of a breach or unauthorized remote activation, what response protocols are in place?
- How do you ensure that the approach to managing remote activation and device usage indications aligns with NIST guidelines and broader cybersecurity objectives?



System and Communications Protection

SC.L2-3.13.11

Derived

Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

- Which cryptographic modules are you currently using to protect the confidentiality of CUI?
- Are these cryptographic modules FIPS 140-2 or FIPS 140-3 validated?
- Can you provide documentation or certification numbers for the FIPS-validated cryptographic modules in use?
- How do you ensure that only FIPS-validated cryptographic methods are employed across all relevant systems and applications?
- How frequently do you review and update cryptographic methods to ensure they align with the latest FIPS standards?
- What processes are in place to handle situations where FIPS validation may be compromised or outdated due to vulnerabilities or advancements in cryptographic attacks?
- How do you train and educate relevant personnel about the importance of using FIPS-validated cryptography for CUI?
- Are there any exceptions or scenarios where non-FIPS validated cryptography is used, and if so, how are they justified and managed?
- How do you ensure third-party vendors, solutions, or integrated systems adhere to FIPS-validated cryptographic standards when handling CUI?
- How do you monitor and verify the correct implementation of FIPS-validated cryptographic modules in real-time operations?
- How do you handle cryptographic key management, generation, storage, and destruction in line with FIPS requirements?

- Are there automated alerts or mechanisms to detect any deviations from FIPS-validated cryptographic standards?
- How do you integrate FIPS-validated cryptography enforcement with other security tools or protocols?
- Describe any challenges or issues you've encountered in implementing or maintaining FIPS-validated cryptography and how they were addressed.
- How do you stay updated on changes or updates to FIPS cryptographic standards?
- How do you test or validate the effectiveness and correct implementation of FIPS-validated cryptographic modules?
- Are there periodic security audits or assessments to verify adherence to FIPS-validated cryptographic practices?
- How do you ensure backup and recovery processes also adhere to FIPS-validated cryptographic standards when dealing with CUI?
- In cases where CUI is transferred or shared externally, how do you ensure the data remains protected with FIPS-validated cryptography?
- How do you ensure that the approach to using FIPS-validated cryptography aligns with the broader NIST guidelines and cybersecurity objectives of the organization?



System and Communications Protection



SC.L2-3.13.10



Derived



Establish and manage cryptographic keys for cryptography employed in organizational systems.

- Describe your organization's process for generating cryptographic keys.
- How do you store and protect private and secret cryptographic keys?
- What mechanisms are in place to ensure the secure distribution and transmission of cryptographic keys?
- How do you handle the lifecycle management of cryptographic keys, including generation, distribution, rotation, and retirement?
- What tools or platforms do you use for cryptographic key management?
- Are there automated alerts or mechanisms in place to detect potential unauthorized access or misuse of cryptographic keys?
- How frequently do you rotate or change cryptographic keys?
- Describe the process for revoking or invalidating cryptographic keys when needed.
- How do you ensure redundancy and backup of critical cryptographic keys?

- What measures are in place to protect cryptographic keys during transit and at rest?
- How do you manage and monitor third-party access to cryptographic keys?
- Describe any hardware security modules (HSMs) or dedicated key management solutions employed.
- How do you handle cryptographic key management for cloud services or external platforms?
- Describe the process for recovering from the loss or compromise of a cryptographic key.
- How do you ensure compliance with industry standards or best practices related to cryptographic key lengths and algorithms?
- How are personnel trained and made aware of their responsibilities related to cryptographic key management?
- Are there periodic security audits or assessments to validate the security and integrity of your cryptographic key management practices?
- How do you address feedback or concerns related to cryptographic key management?
- Describe any challenges or issues you've faced related to cryptographic key management and how they were addressed.
- How do you ensure that your approach to cryptographic key management aligns with NIST guidelines and broader cybersecurity objectives?



System and Communications Protection

SC.L2-3.13.9

Derived

Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

- How does your organization define the criteria for terminating inactive network connections?
- What mechanisms or tools are in place to automatically terminate communications sessions after a set period of inactivity?
- How do you determine the appropriate duration of inactivity before a session is terminated?
- Are there exceptions or specific scenarios where the inactivity threshold might be extended or shortened?
- Describe the processes used to inform users about session termination due to inactivity.
- How do you ensure that the termination of connections doesn't result in data loss or disrupt ongoing operations?
- What protocols are in place for users to re-establish a terminated session safely and securely?
- How do you handle sessions that require prolonged connectivity or are critical in nature?

- Are there automated alerts or mechanisms in place to detect and respond to sessions that bypass the termination criteria?
- How do you integrate session termination with other security measures, such as user authentication or session encryption?
- How do you handle third-party or external connections in terms of session termination due to inactivity?
- Are there different thresholds or protocols for session termination on different types of systems or applications within the organization?
- Describe any challenges or issues you've encountered related to session termination and how they were addressed.
- How do you educate and train users about the importance of session termination and the risks of prolonged inactivity?
- How do you test or validate the effectiveness of your session termination mechanisms?
- How do you manage feedback or concerns from users or departments about session termination protocols?
- How do you stay updated on best practices and industry standards related to session termination and inactivity thresholds?
- Are there periodic security audits or assessments to verify the consistent application of session termination protocols across all systems?
- How do you ensure that the session termination process doesn't inadvertently introduce new vulnerabilities or attack vectors?
- How do you ensure that the approach to terminating network connections due to inactivity aligns with NIST guidelines and broader cybersecurity objectives?



System and Communications Protection



SC.L2-3.13.6



Derived



Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

- How does your organization implement the "deny all, permit by exception" principle for network communications?
- What tools or solutions do you use to enforce this network traffic policy?
- How do you determine which network communications are exceptions and should be permitted?
- Describe the process for requesting and approving exceptions to the default deny policy.
- How frequently are the permitted exceptions reviewed and validated?

- How do you ensure that unauthorized or unexpected network traffic is promptly detected and addressed?
- How do you handle emergency or urgent needs that might require temporary changes to the network traffic policy?
- What measures are in place to educate and inform stakeholders about the “deny all, permit by exception” principle?
- How do you manage third-party or external connections in light of this network traffic policy?
- Are there specific protocols or considerations for managing network traffic in cloud environments or remote access scenarios?
- How do you test or validate the effectiveness of the “deny all, permit by exception” policy in preventing unauthorized network communications?
- Describe any challenges or issues you’ve faced in implementing this network traffic policy and how they were addressed.
- How do you integrate the enforcement of this policy with other security tools or incident response systems?
- How do you ensure that the “deny all, permit by exception” approach doesn’t inadvertently hamper critical business processes or functions?
- Are there automated alerts or mechanisms in place to notify relevant personnel of denied network communication attempts?
- How do you handle feedback or concerns from departments or users about network communication restrictions?
- How do you collaborate with external entities, industry peers, or security experts to enhance your approach to network traffic management?
- Are there periodic audits or assessments to validate the effectiveness and appropriateness of the network traffic exceptions in place?
- How do you ensure continuity in network access and communication during system updates, migrations, or the introduction of new technologies?
- How do you ensure that the approach to network traffic management aligns with the organization’s broader cybersecurity objectives and NIST compliance requirements?



System and Communications Protection



SC.L2-3.13.15



Derived



Protect the authenticity of communications sessions.

- What mechanisms do you employ to ensure the authenticity of communications sessions?
- How do you implement and manage digital signatures or certificates to authenticate communication sessions?
- Describe the protocols and tools in place to prevent man-in-the-middle attacks.
- How do you ensure the authenticity of remote communication sessions, especially those originating from external networks?
- What methods are used to validate the identity of devices or systems involved in a communication session?
- How do you handle communications that fail authenticity checks?
- Describe the process for issuing, renewing, and revoking authentication credentials or certificates.
- How do you ensure secure handshakes between communicating devices or systems?
- Are there automated alerts or mechanisms to detect potential breaches in communication authenticity?
- How do you manage and monitor third-party or partner communication sessions to ensure their authenticity?
- How do you integrate communication session authenticity with other security controls like encryption or intrusion detection?
- How frequently do you review and update your methods and tools for ensuring communication authenticity?
- How do you ensure that communication authenticity mechanisms don't hinder performance or user experience?
- What training or awareness programs are in place to educate users about the importance of communication session authenticity?
- How do you handle legacy systems or older communication protocols in terms of ensuring session authenticity?
- Describe any challenges or issues you've encountered related to communication session authenticity and how they were addressed.
- How do you validate the effectiveness of your mechanisms for ensuring communication authenticity?
- How do you stay informed about emerging threats or vulnerabilities related to communication session authenticity?

- Are there periodic security audits or assessments to validate the effectiveness of your communication authenticity mechanisms?
- How do you ensure that the approach to ensuring communication session authenticity aligns with NIST guidelines and broader cybersecurity objectives?



System and Communications Protection



SC.L1-3.13.5



Derived



Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

- How does your organization implement subnetworks for publicly accessible components?
- Describe the physical or logical separation mechanisms in place between these subnetworks and your internal networks.
- What tools or platforms do you use to manage and monitor these separated subnetworks?
- How do you ensure that traffic between the public subnetworks and internal networks is securely managed and monitored?
- Are there specific security controls or firewalls in place to prevent unauthorized access from the publicly accessible subnetworks to the internal networks?
- How frequently do you review and update the configuration and security measures of these subnetworks?
- Describe the process for granting and managing access between the subnetworks and the internal networks.
- How do you handle potential vulnerabilities or threats detected on the publicly accessible subnetworks?
- How do you ensure that third-party services or components on these subnetworks don't introduce vulnerabilities to the internal networks?
- Are there automated alerts or mechanisms in place to detect and respond to security incidents on the subnetworks?
- How do you manage data flow and storage between publicly accessible subnetworks and internal networks?
- Describe any challenges or issues you've faced related to managing these subnetworks and how they were addressed.
- How do you ensure that the security measures on the subnetworks do not inadvertently hamper legitimate access or functionality?
- How do you handle backup, recovery, and resilience for the publicly accessible subnetworks?

- Are there periodic security audits or assessments to validate the integrity and security of these subnetworks in relation to the internal networks?
- How do you train and educate relevant personnel about the importance and procedures related to managing the separated subnetworks?
- How do you stay updated on best practices and industry standards related to managing publicly accessible subnetworks?
- How do you ensure continuity of service and security during updates, migrations, or changes to the subnetworks?
- How do you handle feedback or concerns from stakeholders or users related to the accessibility or performance of the publicly accessible subnetworks?
- How do you ensure that the approach to managing and separating these subnetworks aligns with NIST guidelines and broader cybersecurity objectives?



System and Communications Protection

SC.L2-3.13.4

Derived

Prevent unauthorized and unintended information transfer via shared system resources.

- How do you manage and monitor access to shared system resources?
- What controls are in place to prevent unauthorized information transfers through shared resources?
- Describe the mechanisms used to segregate data or processes within shared system resources.
- How do you ensure that users can only access and transfer data for which they have permissions in shared environments?
- What tools or platforms are employed to detect and alert on unauthorized information transfers?
- How do you handle shared resources in virtualized or cloud environments to prevent unauthorized data transfers?
- Are there any logging mechanisms specific to shared resource access and data transfers? If so, how frequently are these logs reviewed?
- How do you manage third-party access to shared resources to ensure they don't inadvertently transfer unauthorized information?
- What training or awareness programs are in place to educate users about the risks and protocols related to shared system resources?
- How do you ensure that shared resources, like printers or shared drives, are not misused for unauthorized data transfers?

- Describe any challenges or issues you've faced related to unauthorized transfers in shared resources and how they were addressed.
- How do you test or validate the effectiveness of controls placed on shared system resources?
- Are there specific protocols for highly sensitive data in the context of shared resources?
- How do you manage feedback or concerns from stakeholders related to shared resource access and data transfers?
- How do you handle data remnants or potential data leakage in shared resource environments?
- How do you integrate shared resource controls with other security systems, like Data Loss Prevention (DLP) tools or intrusion detection systems?
- How do you ensure that shared system resources are updated or patched without compromising their data segregation controls?
- Are there periodic security audits or assessments focused on shared resource controls and unauthorized data transfers?
- How do you handle incidents or breaches related to unauthorized data transfers in shared resources?
- How do you ensure that controls on shared system resources align with NIST guidelines and the broader cybersecurity objectives of the organization?



System and Communications Protection

SC.L2-3.13.3

Derived

Separate user functionality from system management functionality.

- How does your organization differentiate between user functionality and system management functionality in its systems and applications?
- What mechanisms are in place to ensure that regular users cannot access system management functions?
- Describe the tools or platforms used to enforce this separation of functionalities.
- How do you ensure that system administrators or those with management functionality cannot perform regular user functions under the same account or session?
- Are there distinct interfaces or portals for users and system administrators?
- How do you handle shared roles or accounts that might need both user and management functionalities?
- How do you audit or monitor access to system management functions to ensure only authorized individuals can use them?
- What training or awareness programs are in place to educate system administrators about the

importance of separating their roles from regular user roles?

- How do you manage third-party or external personnel who might need system management functionalities?
- Describe any challenges or issues you've faced in implementing this separation of functionalities and how they were addressed.
- Are there automated alerts or mechanisms to detect and respond to potential violations of this separation principle?
- How do you integrate the enforcement of this separation with other security measures, such as multi-factor authentication or logging?
- How frequently do you review and refine your approach to separating user and system management functionalities?
- How do you ensure that software updates, patches, or new system implementations adhere to this separation principle?
- Are there specific protocols or measures for critical or sensitive systems to further reinforce this separation?
- How do you handle exceptions or scenarios where temporary overlap of functionalities might be required?
- How do you test or validate the effectiveness of mechanisms enforcing the separation of user and management functionalities?
- How do you stay updated on industry best practices or recommendations related to this separation of functionalities?
- Are there periodic security audits or assessments to ensure consistent and effective separation of user and management functionalities?
- How do you ensure that the approach to separating functionalities aligns with NIST guidelines and the organization's broader cybersecurity objectives?



System and Communications Protection



SC.L2-3.13.2



Basic



Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

- How do your architectural designs incorporate information security principles?
- Describe the software development techniques you employ to ensure system security.
- What systems engineering principles do you utilize to enhance information security within your systems?

- How do you ensure that security is considered in the earliest stages of system design and development?
- Are there specific secure coding practices or guidelines that your development teams follow?
- How do you handle third-party components or software in terms of security design and validation?
- Describe any security frameworks or models that guide your architectural and design decisions.
- How do you ensure that security considerations are consistently applied across different systems or projects?
- What tools or platforms do you use to validate and verify security features during the development phase?
- How do you handle the trade-offs between functionality, performance, and security in system design?
- How do you ensure that security architecture and design considerations evolve with emerging threats and technologies?
- How do you integrate security considerations with other architectural concerns like scalability, availability, and usability?
- Describe any challenges or issues you've faced related to security in system design and how they were addressed.
- How do you collaborate with external entities, industry peers, or security experts on best practices in secure design and development?
- Are there periodic security assessments or reviews focused on architectural and design decisions?
- How do you educate and train your development and engineering teams on secure design principles?
- How do you ensure that legacy systems or existing solutions are aligned with current secure design and development principles?
- How do you manage feedback or concerns related to security implications of system design decisions?
- How do you measure the effectiveness of your security-focused architectural and design practices?
- How do you ensure that the approach to secure design and development aligns with NIST guidelines and the broader cybersecurity objectives of your organization?



System and Communications Protection



SC.L1-3.13.1



Basic



Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

- What mechanisms and tools do you use to monitor communications at the external boundaries of your systems?
- How do you identify and establish key internal boundaries within your organizational systems?
- Describe the controls in place to protect information transmitted across these boundaries.
- How do you ensure the integrity and confidentiality of information during transmission?
- What protocols and technologies are employed for encrypting data in transit?
- How do you detect and respond to unauthorized or suspicious communications at these boundaries?
- Are there specific firewalls, intrusion detection systems, or intrusion prevention systems deployed at these boundaries?
- How frequently are the configurations of these monitoring and control tools reviewed and updated?
- Describe any segmentation or isolation strategies employed to separate sensitive or critical system components.
- How do you manage and control communications involving third-party vendors or external partners?
- Are there automated alerts or mechanisms in place to detect potential breaches or exfiltration attempts?
- How do you ensure that remote access communications are also monitored and protected?
- Describe the process for updating or patching communication protection tools and ensuring they remain effective against evolving threats.
- How do you handle encrypted traffic inspection and management at these boundaries?
- What measures are in place to ensure the availability and resilience of communications, especially during high-traffic periods or potential denial-of-service attacks?
- How do you manage and control wireless communications within and across these boundaries?
- Are there periodic security audits, tests, or assessments to validate the effectiveness of communication protection mechanisms?
- How do you train and educate relevant personnel about the importance and best practices of communication protection?
- Describe any challenges or incidents related to communications protection you've encountered, and how they were addressed.
- How do you ensure that your approach to monitoring, controlling, and protecting communications aligns with NIST guidelines and broader cybersecurity objectives?



System and Communications Protection



SC.L2-3.13.8



Derived



Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

- What cryptographic mechanisms do you currently employ to protect CUI during transmission?
- How do you ensure that these cryptographic mechanisms meet or exceed NIST-approved standards?
- Are there any instances where CUI is transmitted without cryptographic protection? If so, what alternative physical safeguards are in place?
- How do you manage and protect cryptographic keys used for encrypting CUI during transmission?
- How do you ensure that third-party vendors or partners also employ adequate cryptographic protections when transmitting CUI?
- What protocols are in place to handle potential breaches or unauthorized disclosures of CUI during transmission?
- How often do you review and update your cryptographic mechanisms in light of evolving threats and best practices?
- How do you handle legacy systems or platforms that may not support the latest cryptographic standards?
- Describe the training or awareness programs in place to ensure personnel understand the importance of encrypting CUI during transmission.
- How do you validate the effectiveness and integrity of your cryptographic mechanisms?
- What methods are used to ensure secure key exchange or handshakes during encrypted transmissions of CUI?
- How do you handle situations where encrypted CUI transmissions need to be decrypted and inspected for security reasons?
- Are there automated alerts or mechanisms in place to detect potential unauthorized disclosures of CUI during transmission?
- How do you manage the lifecycle of cryptographic keys, including generation, storage, rotation, and disposal?
- Are there specific challenges or issues you've faced related to encrypting CUI during transmission, and how were they addressed?
- How do you stay updated on industry best practices and recommendations related to cryptographic protections for CUI transmission?

- In scenarios where encryption is not feasible, how do you ensure that alternative physical safeguards effectively protect CUI during transmission?
- How do you ensure compatibility and secure transmission of CUI when dealing with external entities or systems that might use different cryptographic standards or mechanisms?
- Are there periodic security audits or assessments to validate the consistent and effective encryption of CUI during transmission?
- How do you ensure that the approach to encrypting CUI during transmission aligns with NIST guidelines and the organization's broader cybersecurity objectives?



System and Communications Protection



SC.L2-3.13.16



Derived



Protect the confidentiality of CUI at rest.

- What encryption methods do you employ to protect CUI when it's stored or at rest?
- How do you determine where CUI is stored within your organization's systems and databases?
- How frequently do you audit and verify the encryption of CUI at rest?
- What measures are in place to detect and respond to unauthorized access attempts to stored CUI?
- How do you manage encryption keys, and what is their lifecycle?
- Are there specific standards or protocols that you adhere to for encrypting CUI at rest?
- How do you ensure that backups or replicas of CUI data are also encrypted and protected?
- What access controls are in place to restrict access to CUI storage locations?
- How do you handle decommissioning or disposal of storage devices containing CUI to ensure data confidentiality?
- Are there any exceptions or scenarios where CUI might be stored without encryption? If so, how are they justified and managed?
- How do you ensure third-party vendors or cloud service providers adhere to your standards for protecting CUI at rest?
- Describe any challenges or issues you've faced related to protecting CUI at rest and how they were addressed.
- How do you handle cases where encryption of CUI at rest might affect data accessibility or system performance?
- How do you stay updated on best practices and industry standards related to protecting CUI at rest?
- Are there periodic security audits or assessments to validate the protection of CUI at rest?

- How do you train and educate relevant personnel on the importance and methods of protecting CUI at rest?
- How do you ensure redundancy and availability of CUI data while maintaining its confidentiality at rest?
- How do you integrate protection measures for CUI at rest with other security tools or data management systems?
- How do you manage and monitor logs related to access and modifications of stored CUI?
- How do you ensure that your approach to protecting CUI at rest 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.







40 Burton Hills Blvd
Suite 200
Nashville, TN 37215

info@redspin.com
www.redspin.com

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.

Key

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

Security Requirement Table of Contents

System and Information Integrity

- Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.....4
- Update malicious code protection mechanisms when new releases are available.....5
- Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.....6
- Provide protection from malicious code at designated locations within organizational systems.....7
- Identify, report, and correct system flaws in a timely manner.....8
- Monitor system security alerts and advisories and take action in response.....9
- Identify unauthorized use of organizational systems.....10

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.



40 Burton Hills Blvd
Suite 200
Nashville, TN 37215

info@redspin.com
www.redspin.com