





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