





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