GUIDE

Redspin
A Division of Clearwater

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.

TABLE OF CONTENTS

Key

Domain Family

Identifier

Basic | Derived

Security Requirement

Security Requirement Table of Contents

As you prepare for your organization's assessment, it's important to understand what to expect during the interview process. Individuals can anticipate a range of questions that will be both comprehensive and reflective of several key areas intended to assure that the controls are implemented correctly and performing as expected. Interview sessions typically follow a basic pattern to help inform this decision. Below is an example interview session construct. Though not all inclusive these guides provide typical questions asked during an assessment.

Typical Question Format:

Policy and Procedures:

- How does your organization's security policy address the encryption of Controlled Unclassified Information (CUI) on mobile devices and platforms?
- Can you provide documentation or guidelines that mandate encryption on mobile devices and platforms when handling CUI?

Implementation:

- What encryption standards or protocols does your organization use for CUI on mobile devices?
- Are there specific mobile device management (MDM) or mobile application management (MAM) tools in place to enforce encryption on mobile devices and platforms?
- How do you ensure that all mobile devices used within the organization have encryption enabled?

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.

Redspin
A Division of Clearwater

40 Burton Hills Blvd
Suite 200
Nashville, TN 37215

info@redspin.com
www.redspin.com