GUIDE

Redspin
A Division of Clearwater

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

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

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

TABLE OF CONTENTS

Key

Domain Family

Identifier

Basic | Derived

Security Requirement

Security Requirement Table of Contents

Audit and Accountability

- Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.....4
- Limit management of audit logging functionality to a subset of privileged users.....5
- Protect audit information and audit logging tools from unauthorized access, modification, and deletion.....6
- Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.....7
- Provide audit record reduction and report generation to support on-demand analysis and reporting.....8
- Alert in the event of an audit logging process failure.....9
- Review and update logged events.....10
- Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.....11
- Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.....12

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

Typical Question Format:

Policy and Procedures:

- How does your organization's security policy address the encryption of Controlled Unclassified Information (CUI) on mobile devices and platforms?

- Can you provide documentation or guidelines that mandate encryption on mobile devices and platforms when handling CUI?

Implementation:

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

Monitoring and Auditing:

- How do you monitor and verify that CUI remains encrypted on mobile devices and platforms?
- Are there any auditing mechanisms in place to check for devices that might have encryption disabled or bypassed?
- Can you provide recent audit logs or reports showing encryption checks for mobile devices?

Incident Handling:

- Have there been any incidents where CUI was found unencrypted on a mobile device? If so, how was it handled?
- What are the consequences or actions taken against users who fail to encrypt CUI on their mobile devices?

Training and Awareness:

- How are employees made aware of the importance of encrypting CUI on mobile devices?
- Is there a specific training module or awareness campaign focused on mobile device encryption?

Technical:

- Can you demonstrate the encryption settings on a sample mobile device used within the organization?
- Are there any exceptions or scenarios where CUI might not be encrypted on mobile devices, and how are these exceptions handled?

Third-party and BYOD:

- How does your organization ensure that third-party vendors or contractors adhere to this encryption requirement when accessing CUI on mobile devices?
- If you have a Bring Your Own Device (BYOD) policy, how do you ensure that personal devices encrypt CUI?

Audit and Accountability

AU.L2-3.3.5

Derived

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

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

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

Audit and Accountability

AU.L2-3.3.9

Derived

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

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

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

Audit and Accountability

AU.L2-3.3.8

Derived

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

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

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

Audit and Accountability

AU.L2-3.3.7

Derived

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

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

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

Audit and Accountability

AU.L2-3.3.6

Derived

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

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

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

Audit and Accountability

AU.L2-3.3.4

Derived

Alert in the event of an audit logging process failure.

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

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

Audit and Accountability

AU.L2-3.3.3

Derived

Review and update logged events.

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

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

Audit and Accountability

AU.L2-3.3.2

Basic

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

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

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

Audit and Accountability

AU.L2-3.3.1

Basic

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

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

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

WHY REDSPIN

- Over 100 security advisors and assessors, ready to scale with you as needed
- Possesses the know-how from performing over 1,000 assessments in highly regulated industries, including multiple Joint Surveillance Voluntary Assessment Program (JSVAP) assessments
- Uplifts its service offering to validate your security, giving you the confidence that your people, processes, and technology are effective
- Our team understands CMMC requirements and follows professional conduct to help you on your journey to becoming CMMC-ready and certified

Redspin, a division of Clearwater, has become one of the most trusted cybersecurity companies for the Defense Industrial Base. Our exclusive focus on tailoring our CMMC assessment, training, consulting, and managed services for each client delivers peace of mind by lowering the risk of a security incident or breach, and meeting/maintaining compliance regulations. Since our founding in 2001, we've become a thought leader in IT security, helped countless clients control their security risk, develop their security strategy, and avoid a breach headline.

Redspin
A Division of Clearwater

40 Burton Hills Blvd
Suite 200
Nashville, TN 37215

info@redspin.com
www.redspin.com