Strike Graph

CMMC SSP

System Security Plan Template

Prepared for:

Last updated:

1. System Identification

1.1. System Name/Title: [State the name of the system. Spell out acronyms.]

1.1.1. System Categorization: Moderate Impact for Confidentiality

1.1.2. System Unique Identifier: [Insert the System Unique Identifier]

1.2. Responsible Organization:

Name:	
Address:	
Phone:	

1.2.1. Information Owner (Government point of contact responsible for providing and/or receiving CUI):

Name:	
Title:	
Office Address:	
Work Phone:	
E-mail Address:	

1.2.2. System Owner (assignment of security responsibility):

Name:	
Title:	
Office Address:	
Work Phone:	
E-mail Address:	

1.2.2.1. System Security Officer:

Name:	
Title:	
Office Address:	
Work Phone:	
E-mail Address:	

1.3. **General Description/Purpose of System:** What is the function/purpose of the system? [Provide a short, high-level description of the function/purpose of the system.]

1.3.1. Number of end users and privileged users: [In the table below, provide the approximate number of users and administrators of the system. Include all those with privileged access such as system administrators, database administrators, application administrators, etc. Add rows to define different roles as needed.]

Roles of Users and Number of Each Type:

Number of Users	Number of Administrators/ Privileged Users

1.4. **General Description of Information:** CUI information types processed, stored, or transmitted by the system are determined and documented. For more information, see the CUI Registry at https://www.archives.gov/cui/registry/category-list.

[Document the CUI information types processed, stored, or transmitted by the system below].

2. System Environment

Include a detailed topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and key devices. (Note: this does not require depicting every workstation or desktop, but include an instance for each operating system in use, an instance for portable components (if applicable), all virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations (e.g., Unix, Windows, Mac, Linux), firewalls, routers, switches, copiers, printers, lab equipment, handhelds). If components of other systems that interconnect/ interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram. Insert a system topology graphic. Provide a narrative consistent with the graphic that clearly lists and describes each system component.]

2.1. Include or reference a complete and accurate listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component.

Hardware	Type	Purpose

2.2. List all software components installed on the system.

Software	Purpose

2.3. Hardware and Software Maintenance and Ownership - Is all hardware and software maintained and owned by the organization? □ Yes □ No

If no, explain:

3. Requirements

(Note: The source of the requirements is NIST Special Publication 800-171, dated December 2016)

Provide a thorough description of how all of the security requirements are being implemented or planned to be implemented. The description for each security requirement contains: 1) the security requirement number and description; 2) how the security requirement is being implemented or planned to be implemented; and 3) any scoping guidance that has been applied (e.g., compensating mitigations(s) in place due to implementation constraints in lieu of the stated requirement). If the requirement is not applicable to the system, provide rationale.

3.1. Family: Access Control (AC)

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

Assessment Objective:

Determine if:
[a] authorized users are identified.
[b] processes acting on behalf of authorized users are identified.
[c] devices (and other systems) authorized to connect to the system are identified.
[d] system access is limited to authorized users.
[e] system access is limited to processes acting on behalf of authorized users.
[f] system access is limited to authorized devices (including other systems).

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must implement strict access controls ensuring only approved users, devices, and processes can connect to systems. Evidence may include access control lists, onboarding/offboarding procedures, and device authorization logs. Pitfalls include failing to promptly remove access for departing staff or overlooking service accounts.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] the types of transactions and functions that authorized users are permitted to execute are defined.
[b] system access is limited to the defined types of transactions and functions for authorized users.

Status:	□ Implemented	□ Planned	□ Not Applicable

Strike Graph Guidance: Organizations must restrict user permissions to match job responsibilities, enforcing least privilege for functions and transactions. Evidence may include role-based access control (RBAC) policies, privilege review logs, and screenshots of access matrices. Common pitfalls include role creep (users accumulating privileges over time) or failing to periodically review permissions.

[Click here to type your detailed process]

3.1.3. Control the flow of CUI in accordance with approved authorizations.

Assessment Objective:

Determine if:
[a] information flow control policies are defined.
[b] methods and enforcement mechanisms for controlling the flow of CUI are defined.
[c] designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.
[d] authorizations for controlling the flow of CUI are defined. 3.1.3[e] approved authorizations for controlling the flow of CUI are enforced.

Status:	□ Implemented	□ Planned	□ Not Applicable

Strike Graph Guidance: Organizations must document and enforce approved rules for how Controlled Unclassified Information (CUI) flows within and between systems. Evidence may include network diagrams, firewall or proxy configurations, and DLP (Data Loss Prevention) policies. Pitfalls include undocumented transfers, shadow IT solutions, or relying on unencrypted email for CUI.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] the duties of individuals requiring separation are defined.
[b] responsibilities for duties that require separation are assigned to separate individuals.

[c] access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must enforce segregation of duties so no single person can complete high-risk actions alone. Evidence may include workflow charts, separation of financial and system administration roles, and audit trails showing multi-person approvals. Pitfalls include small teams where the same individual performs conflicting roles or bypassing dual-control processes.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] privileged accounts are identified.
[b] access to privileged accounts is authorized in accordance with the principle of least privilege.
[c] security functions are identified.
[d] access to security functions is authorized in accordance with the principle of least privilege.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must assign only the minimum rights necessary for users and administrators to perform their roles. Evidence may include role-based access control documentation, admin role assignments, and privilege audit reports. Pitfalls include granting blanket administrator rights, leaving default admin accounts enabled, or failing to re-certify access regularly.

[Click here to type your detailed process]

3.1.6. Use non-privileged accounts or roles when accessing nonsecurity functions.

Assessment Objective:

Determine if:
[a] nonsecurity functions are identified.
[b] users are required to use non-privileged accounts or roles when accessing nonsecurity functions.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must require staff to use standard, non-privileged accounts for day-to-day business functions, reserving admin accounts strictly for security tasks. Evidence may include user account policies, AD group membership records, and login session reviews. Pitfalls include staff habitually using admin accounts for routine work or failing to disable inactive privileged accounts.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] privileged functions are defined.
[b] non-privileged users are defined.
[c] non-privileged users are prevented from executing privileged functions.
[d] the execution of privileged functions is captured in audit logs.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must enforce technical restrictions so non-privileged accounts cannot execute admin-level commands, while ensuring all privileged activity is logged. Evidence may include audit logs showing privileged command execution, system security configurations, and access denial events. Pitfalls include misconfigured logging that omits admin actions or over-reliance on manual monitoring.

[Click here to type your detailed process]

3.1.8. Limit unsuccessful logon attempts.

Assessment Objective:

Determine if:
[a] the means of limiting unsuccessful logon attempts is defined.
[b] the defined means of limiting unsuccessful logon attempts is implemented.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must enforce account lockout thresholds after a set number of failed logon attempts to reduce brute force attack risk. Evidence may include screenshots of lockout policy settings, SIEM alerts for repeated failures, and account lockout reports. Pitfalls include setting thresholds too high, exempting privileged accounts, or failing to alert administrators of lockout events.

[Click here to type your detailed process]

3.1.9. Provide privacy and security notices consistent with applicable CUI rules.

Assessment Objective:

Determine if:
[a] privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category.
[b] privacy and security notices are displayed.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must display privacy and security notices that align with CUI handling requirements at system access points. Evidence may include login banner configurations, screenshots of system warnings, and documented notice text. Pitfalls include outdated banners that reference incorrect policies or inconsistent application across systems.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] the period of inactivity after which the system initiates a session lock is defined.
[b] access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity.
[c] previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must configure systems to automatically lock after inactivity, hiding sensitive information until re-authentication. Evidence may include workstation group policy settings, screenshots of lock screen configurations, and audit logs of session lock events. Pitfalls include excessive lockout times or users disabling locks through local settings.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] conditions requiring a user session to terminate are defined.
[b] a user session is automatically terminated after any of the defined conditions occur.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must configure systems to end user sessions after defined triggers, such as timeout periods or detected anomalies. Evidence may include system timeout policies, termination configuration settings, and logs showing ended sessions. Pitfalls include relying solely on user-driven logouts or inconsistent enforcement across applications.

[Click here to type your detailed process]

3.1.12. Monitor and control remote access sessions.

Assessment Objective:

Determine if:
[a] remote access sessions are permitted.
[b] the types of permitted remote access are identified.
[c] remote access sessions are controlled.
[d] remote access sessions are monitored.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must actively monitor and restrict remote access, ensuring only authorized connections are maintained. Evidence may include VPN logs, remote session monitoring dashboards, and policies detailing approved remote access methods. Pitfalls include allowing split tunneling, failing to record remote activity, or using unapproved remote tools.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] cryptographic mechanisms to protect the confidentiality of remote access sessions are identified.
[b] cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must use strong encryption (such as TLS or IPsec) to protect all remote access sessions carrying CUI. Evidence may include VPN configuration files, encryption protocol settings, and penetration test results verifying encrypted channels. Pitfalls include allowing legacy protocols, weak ciphers, or misconfigured certificates.

[Click here to type your detailed process]

3.1.14. Route remote access via managed access control points.

Assessment Objective:

Determine if:
[a] managed access control points are identified and implemented.
[b] remote access is routed through managed network access control points.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must ensure all remote access traffic flows through secure, centrally managed gateways. Evidence may include network architecture diagrams, firewall rules, and VPN concentrator configurations. Pitfalls include users bypassing gateways with direct connections or failing to monitor access control point logs.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] privileged commands authorized for remote execution are identified.
[b] security-relevant information authorized to be accessed remotely is identified.
[c] the execution of the identified privileged commands via remote access is authorized.
[d] access to the identified security-relevant information via remote access is authorized.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must restrict and formally authorize remote execution of administrative commands or access to sensitive security data. Evidence may include privileged access management (PAM) approvals, session recordings, and access request logs. Pitfalls include blanket remote admin rights or failing to document approval workflows.

[Click here to type your detailed process]

3.1.16. Authorize wireless access prior to allowing such connections.

Assessment Objective:

Determine if:
[a] wireless access points are identified.
[b] wireless access is authorized prior to allowing such connections.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must formally approve and document all wireless connections before they are enabled. Evidence may include wireless access authorization forms, network access control (NAC) configurations, and approval records. Pitfalls include allowing ad hoc wireless access points (rogue APs) or failing to periodically review authorized devices.

[Click here to type your detailed process]

3.1.17. Protect wireless access using authentication and encryption.

Assessment Objective:

Determine if:
[a] wireless access to the system is protected using authentication.
[b] wireless access to the system is protected using encryption.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must secure all wireless networks with strong authentication methods and encryption standards (e.g., WPA3). Evidence may include wireless security policies, configuration screenshots, and vulnerability scans verifying encryption strength. Pitfalls include using weak encryption protocols like WEP/WPA or leaving default SSIDs/passwords unchanged.

[Click here to type your detailed process]

3.1.18. Control connection of mobile devices.

Assessment Objective:

Determine if:
[a] mobile devices that process, store, or transmit CUI are identified.
[b] mobile device connections are authorized.
[c] mobile device connections are monitored and logged.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must define and enforce policies for mobile device usage, ensuring only compliant and authorized devices connect to systems. Evidence may include mobile device management (MDM) enrollment records, compliance reports, and access logs. Pitfalls include unmanaged BYOD devices, missing encryption on mobile platforms, or failing to revoke access for lost devices.

[Click here to type your detailed process]

3.1.19. Encrypt CUI on mobile devices and mobile computing platforms.

Assessment Objective:

Determine if:
[a] mobile devices and mobile computing platforms that process, store, or transmit CUI are identified.
[b] encryption is employed to protect CUI on identified mobile devices and mobile computing platforms.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must ensure all Controlled Unclassified Information (CUI) stored on mobile devices is encrypted with FIPS-validated algorithms. Evidence may include MDM configuration policies, device encryption status reports, and screenshots verifying encryption enforcement. Pitfalls include allowing exceptions for certain devices, using weak encryption standards, or failing to encrypt removable media.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] connections to external systems are identified.
[b] the use of external systems is identified.
[c] connections to external systems are verified.
[d] the use of external systems is verified.
[e] connections to external systems are controlled/limited.
[f] the use of external systems is controlled/limited.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must regulate and monitor any connections to external systems to prevent unauthorized transfer of CUI. Evidence may include firewall rules, VPN connection logs, and access request forms for external systems. Pitfalls include granting broad access without review, failing to log external activity, or neglecting to remove access when external relationships end.

[Click here to type your detailed process]

3.1.21. Limit use of portable storage devices on external systems.

Assessment Objective:

Determine if:
[a] the use of portable storage devices containing CUI on external systems is identified and documented.
[b] limits on the use of portable storage devices containing CUI on external systems are defined.
[c] the use of portable storage devices containing CUI on external systems is limited as defined.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must control and restrict the use of portable storage devices (like USB drives) when connected to external systems. Evidence may include device control policies, endpoint management logs, and removable media usage reports. Pitfalls include failing to disable unused ports, not encrypting approved storage devices, or neglecting to monitor device usage.

[Click here to type your detailed process]

3.1.22. Control information posted or processed on publicly accessible systems.

Assessment Objective:

Determine if:
[a] individuals authorized to post or process information on publicly accessible systems are identified.
[b] procedures to ensure CUI is not posted or processed on publicly accessible systems are identified.
[c] a review process is in place prior to posting of any content to publicly accessible systems.
[d] content on publicly accessible systems is reviewed to ensure that it does not include CUI.
[e] mechanisms are in place to remove and address improper posting of CUI.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must restrict and monitor the posting of CUI or sensitive data on publicly accessible websites or portals. Evidence may include content approval workflows, monitoring of public-facing systems, and training records on data posting policies. Pitfalls include staff posting sensitive data without review or failing to regularly audit public content.

[Click here to type your detailed process]

3.2. Family: Awareness & Training (AT)

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

Assessment Objective:

Determine if:
[a] security risks associated with organizational activities involving CUI are identified.
[b] policies, standards, and procedures related to the security of the system are identified.
[c] managers, systems administrators, and users of the system are made aware of the security risks associated with their activities.
[d] managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must provide regular awareness programs to communicate security risks, responsibilities, and applicable policies to all system users. Evidence may include training materials, attendance records, signed acknowledgment forms, and intranet postings of policies. Pitfalls include one-time training without refreshers or not tailoring content to different roles.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] information security-related duties, roles, and responsibilities are defined.
[b] information security-related duties, roles, and responsibilities are assigned to designated personnel.
[c] personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must deliver job-specific training that equips personnel to handle their security responsibilities effectively. Evidence may include course completion certificates, records of specialized training for admins or developers, and training plans mapped to job roles. Pitfalls include generic training that doesn't address role-specific duties or failing to track completion status.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] potential indicators associated with insider threats are identified.
[b] security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must provide awareness training that helps personnel recognize and report potential insider threat indicators, such as repeated policy violations, unusual system access, or attempts to bypass controls. Evidence may include course materials, completion records, reporting procedures, and awareness campaign artifacts. Pitfalls include one-time training with no refreshers, vague examples that don't resonate with job roles, or failure to establish clear reporting channels.

[Click here to type your detailed process]

3.3. Family: Audit & Accountability (AU)

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

Assessment Objective:

Determine if:
[a] audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.
[b] the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.
[c] audit records are created (generated).
[d] audit records, once created, contain the defined content.
[e] retention requirements for audit records are defined.
[f] audit records are retained as defined.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must generate and securely retain audit logs that capture critical security events for investigation and reporting. Evidence may include SIEM configurations, log retention policies, and stored log files. Pitfalls include retaining logs for too short a period, failing to centralize them, or not protecting them against tampering.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] the content of the audit records needed to support the ability to uniquely trace users to their actions is defined.
[b] audit records, once created, contain the defined content.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must configure systems so that all user activities are uniquely attributable to specific individuals. Evidence may include user account management records, unique ID assignments, and audit logs correlating actions to IDs. Pitfalls include shared accounts without accountability or weak logging that omits critical user actions.

[Click here to type your detailed process]

3.3.3. Review and update logged events.

Assessment Objective:

Determine if:
[a] a process for determining when to review logged events is defined.
[b] event types being logged are reviewed in accordance with the defined review process.
[c] event types being logged are updated based on the review.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must periodically review what events are logged and adjust configurations to maintain relevance. Evidence may include event review meeting notes, updated logging policies, and configuration change records. Pitfalls include outdated logging settings that miss emerging threats or logging excessive irrelevant events that obscure critical activity.

[Click here to type your detailed process]

3.3.4. Alert in the event of an audit logging process failure.

Assessment Objective:

Determine if:
[a] personnel or roles to be alerted in the event of an audit logging process failure are identified.
[b] types of audit logging process failures for which alert will be generated are defined.
[c] identified personnel or roles are alerted in the event of an audit logging process failure.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must configure systems to generate real-time alerts when audit logging processes fail or are disabled. Evidence may include SIEM alert configurations, sample alert messages, and monitoring dashboards. Pitfalls include failing to alert administrators promptly or ignoring alert thresholds for critical systems.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined.
[b] defined audit record review, analysis, and reporting processes are correlated.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must integrate audit record reviews with incident response to detect and act on suspicious activity quickly. Evidence may include correlation rules, incident response reports tied to audit logs, and workflow documentation. Pitfalls include siloed teams that fail to share audit findings or delays in escalating abnormal events.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] an audit record reduction capability that supports on-demand analysis is provided.
[b] a report generation capability that supports on-demand reporting is provided.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must implement tools that summarize and generate reports from audit data to support investigations. Evidence may include SIEM dashboards, automated report templates, and examples of generated reports. Pitfalls include relying solely on raw logs without analysis tools or failing to customize reports for relevant stakeholders.

[Click here to type your detailed process]

3.3.7. Provide an individual (or role) with responsibility for audit review, analysis, and reporting.

Assessment Objective:

Determine if:
[a] internal system clocks are used to generate time stamps for audit records.
[b] an authoritative source with which to compare and synchronize internal system clocks is specified.
[c] internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must formally assign responsibility for reviewing and analyzing audit records to a designated role or team. Evidence may include role descriptions, signed responsibility assignments, and audit review schedules. Pitfalls include unclear ownership of audit review duties or assuming automated tools replace human oversight.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] audit information is protected from unauthorized access.
[b] audit information is protected from unauthorized modification.
[c] audit information is protected from unauthorized deletion.
[d] audit logging tools are protected from unauthorized access.
[e] audit logging tools are protected from unauthorized modification.
[f] audit logging tools are protected from unauthorized deletion.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must secure audit logs and logging tools with access controls that prevent tampering or unauthorized use. Evidence may include access control lists, backup records, and monitoring alerts for unauthorized changes. Pitfalls include storing logs on unprotected servers or granting broad admin rights without separation of duties.

[Click here to type your detailed process]

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

Assessment Objectives

Determine if:
[a] a subset of privileged users granted access to manage audit logging functionality is defined.
[b] management of audit logging functionality is limited to the defined subset of privileged users.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must restrict the ability to configure or disable audit logging to a minimal, trusted set of privileged accounts. Evidence may include privileged user lists, PAM (Privileged Access Management) system records, and screenshots of role-based restrictions. Pitfalls include excessive numbers of privileged users or failure to review permissions regularly.

[Click here to type your detailed process]

3.3.10. Family: Configuration Management (CM)

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

Assessment Objective:

Determine if:
[a] a baseline configuration is established.
[b] the baseline configuration includes hardware, software, firmware, and documentation.
[c] the baseline configuration is maintained (reviewed and updated) throughout the system development life cycle.
[d] a system inventory is established.
[e] the system inventory includes hardware, software, firmware, and documentation.
[f] the inventory is maintained (reviewed and updated) throughout the system development life cycle.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must define and maintain approved baseline configurations and inventories of all system components. Evidence may include baseline configuration documents, inventory management databases, and configuration change logs. Pitfalls include failing to update baselines after major changes or maintaining incomplete inventories that omit firmware or documentation.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] security configuration settings for information technology products employed in the system are established and included in the baseline configuration.
[b] security configuration settings for information technology products employed in the system are enforced.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must implement standard security configurations for all IT products, aligning with industry or vendor benchmarks (e.g., CIS, DISA STIGs). Evidence may include configuration checklists, automated compliance scan reports, and secure baseline templates. Pitfalls include relying on default vendor settings or inconsistent application across systems.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] changes to the system are tracked.
[b] changes to the system are reviewed.
[c] changes to the system are approved or disapproved.
[d] changes to the system are logged.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must manage system changes through a documented change control process requiring tracking, review, approval, and logging. Evidence may include change request tickets, CAB (Change Advisory Board) meeting notes, and system change logs. Pitfalls include making emergency changes without approvals, weak documentation of change rationale, or failing to capture all changes in logs.

[Click here to type your detailed process]

3.3.14. Analyze the security impact of changes prior to implementation.

Assessment Objective:

Determine if the security impact of changes to the system is analyzed prior to implementation.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must assess the potential security effects of all proposed changes before implementation. Evidence may include risk assessment reports, documented security impact analyses, and approval workflows tied to change requests. Pitfalls include skipping impact analysis for urgent changes or treating security as an afterthought in the change process.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] physical access restrictions associated with changes to the system are defined.
[b] physical access restrictions associated with changes to the system are documented.3.4.5[c] physical access restrictions associated with changes to the system are approved.
[d] physical access restrictions associated with changes to the system are enforced.
[e] logical access restrictions associated with changes to the system are defined.
[f] logical access restrictions associated with changes to the system are documented.
[g] logical access restrictions associated with changes to the system are approved.
[h] logical access restrictions associated with changes to the system are enforced.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must formally restrict who can make system changes, both physically and logically, with documented approvals. Evidence may include access control policies, change approval logs, and monitoring reports on privileged actions. Pitfalls include granting broad change rights without review or failing to document exceptions.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] essential system capabilities are defined based on the principle of least functionality.
[b] the system is configured to provide only the defined essential capabilities.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must disable unnecessary services, ports, and functions to reduce attack surfaces. Evidence may include secure configuration baselines, vulnerability scan results, and screenshots of disabled services. Pitfalls include leaving default services enabled or failing to re-apply hardening after system updates.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] essential programs are defined.
[b] the use of nonessential programs is defined.
[c] the use of nonessential programs is restricted, disabled, or prevented as defined.
[d] essential functions are defined.
[e] the use of nonessential functions is defined.
[f] the use of nonessential functions is restricted, disabled, or prevented as defined.
[g] essential ports are defined.
[h] the use of nonessential ports is defined.
[i] the use of nonessential ports is restricted, disabled, or prevented as defined.
[j] essential protocols are defined.
[k] the use of nonessential protocols is defined.
[l] the use of nonessential protocols is restricted, disabled, or prevented as defined.
[m] essential services are defined.
[n] the use of nonessential services is defined.
[o] the use of nonessential services is restricted, disabled, or prevented as defined.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must continuously review systems and restrict or disable unnecessary features and services to minimize attack surfaces. Evidence may include vulnerability scan reports, configuration management records, and system hardening checklists. Pitfalls include leaving default ports open, not disabling unused accounts, or failing to review settings after updates.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] a policy specifying whether whitelisting or blacklisting is to be implemented is specified.
[b] the software allowed to execute under whitelisting or denied use under blacklisting is specified.
[c] whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must implement application control mechanisms that block unauthorized software while allowing only approved applications. Evidence may include application whitelisting policies, EDR configurations, and blocked software reports. Pitfalls include relying only on antivirus tools, failing to review and update allow/deny lists, or granting users override privileges.

[Click here to type your detailed process]

3.3.19. Control and monitor user-installed software.

Assessment Objective:

Determine if:
[a] a policy for controlling the installation of software by users is established.
[b] installation of software by users is controlled based on the established policy.
[c] installation of software by users is monitored.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must prohibit or strictly regulate user-installed software and monitor systems for unauthorized applications. Evidence may include endpoint management logs, application inventory reports, and user software request forms. Pitfalls include allowing unrestricted software installations, lack of monitoring, or inadequate enforcement of software policies.

[Click here to type your detailed process]

3.4. Family: Identification & Authentication (IA)

3.4.1. Identify system users, processes acting on behalf of users, or devices.

Assessment Objective:

Determine if:
[a] system users are identified.
[b] processes acting on behalf of users are identified.
[c] devices accessing the system are identified.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must establish unique identifiers for all users, devices, and processes accessing systems. Evidence may include user account directories, device enrollment records, and service account documentation. Pitfalls include shared accounts, missing device identifiers, or failing to track service accounts.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] the identity of each user is authenticated or verified as a prerequisite to system access.
[b] the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access.
[c] the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must enforce strong authentication mechanisms for users, devices, and processes before granting system access. Evidence may include MFA configuration screenshots, device authentication certificates, and system authentication logs. Pitfalls include using only weak passwords, not requiring MFA for privileged accounts, or bypassing authentication for internal devices.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] privileged accounts are identified.
[b] multifactor authentication is implemented for local access to privileged accounts.
[c] multifactor authentication is implemented for network access to privileged accounts.
[d] multifactor authentication is implemented for network access to non-privileged accounts.

Status: ☐ Implemented ☐ Planned ☐ Not Applicable

Strike Graph Guidance: Organizations must enforce multifactor authentication (MFA) for privileged and standard accounts, whether local or remote. Evidence may include MFA enrollment logs, authentication policy documents, and login screen captures showing MFA enforcement. Pitfalls include enabling MFA only for remote access, leaving privileged service accounts exempt, or failing to monitor MFA bypass attempts.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if replay-resistant authentication mechanisms are implemented for network account access to privileged and non-privileged accounts.

Status: ☐ Implemented ☐ Planned ☐ Not Applicable

Strike Graph Guidance: Organizations must configure authentication protocols to resist replay attacks (e.g., Kerberos, PKI, or token-based systems). Evidence may include authentication configuration files, protocol documentation, and penetration test reports. Pitfalls include reliance on plaintext credentials, legacy protocols without replay protection, or disabling replay-resistance for convenience.

[Click here to type your detailed process]

3.4.5. Prevent reuse of identifiers for a defined period.

Assessment Objective:

Determine if:
[a] a period within which identifiers cannot be reused is defined.
[b] reuse of identifiers is prevented within the defined period.

Status: ☐ Implemented ☐ Planned ☐ Not Applicable

Strike Graph Guidance: Organizations must enforce policies that restrict the reuse of user identifiers (usernames) for a defined retention period. Evidence may include account management policies, identity management system configurations, and user provisioning logs. Pitfalls include failing to define retention periods or allowing rapid reuse of IDs that enable impersonation.

[Click here to type your detailed process]

3.4.6. Disable identifiers after a defined period of inactivity.

Assessment Objective:

Determine if:
[a] a period of inactivity after which an identifier is disabled is defined.
[b] identifiers are disabled after the defined period of inactivity.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must automatically disable inactive accounts after a set period to reduce risk. Evidence may include account disablement policies, automated scripts or system settings, and identity management logs. Pitfalls include exempting privileged accounts, inconsistent enforcement across systems, or failing to notify account owners before deactivation.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] password complexity requirements are defined.
[b] password change of character requirements are defined.
[c] minimum password complexity requirements as defined are enforced when new passwords are created.
[d] minimum password change of character requirements as defined are enforced when new passwords are created.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must implement policies enforcing complex password creation and changes to character sequences when passwords are reset.

Evidence may include password policy configurations, screenshots from directory services, and password audit reports. Pitfalls include overly simplistic requirements, not enforcing complexity on service accounts, or users reusing old passwords.

[Click here to type your detailed process]

3.4.8. Prohibit password reuse for a specified number of generations.

Assessment Objective:

Determine if:
[a] the number of generations during which a password cannot be reused is specified.
[b] reuse of passwords is prohibited during the specified number of generations.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must enforce technical controls preventing users from reusing previous passwords within a defined history count. Evidence may include Active Directory or IAM system password settings, audit logs, and screenshots of password policy configurations. Pitfalls include leaving password history disabled or setting the reuse limit too low to be effective.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if an immediate change to a permanent password is required when a temporary password is used for system logon.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must issue temporary passwords only for initial access and require immediate change upon login. Evidence may include help desk ticketing records, password reset procedures, and logs showing temporary credential changes. Pitfalls include leaving temporary accounts active for extended periods or failing to enforce immediate change at first use.

[Click here to type your detailed process]

3.4.10. Store and transmit only cryptographically-protected passwords.

Assessment Objective:

Determine if:
[a] passwords are cryptographically protected in storage.
[b] passwords are cryptographically protected in transit.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must ensure that all stored and transmitted passwords are cryptographically protected using strong, FIPS-validated methods. Evidence may include IAM system documentation, database encryption settings, and penetration test results confirming encrypted transmission. Pitfalls include storing passwords in plaintext, using weak hashing algorithms, or failing to encrypt backup copies.

[Click here to type your detailed process]

3.4.11. Obscure feedback of authentication information.

Assessment Objective:

Determine if authentication information is obscured during the authentication process.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must configure systems to hide or mask authentication information (e.g., password fields) during entry and login attempts. Evidence may include screenshots of login screens, system configuration settings, and security design documentation. Pitfalls include displaying cleartext passwords during input or error messages that reveal details about credentials.

[Click here to type your detailed process]

3.5. Family: Incident Response (IR)

3.5.1. Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

Assessment Objective:

Determine if:
[a] an operational incident-handling capability is established.

[b] the operational incident-handling capability includes preparation.
[c] the operational incident-handling capability includes detection.
[d] the operational incident-handling capability includes analysis.
[e] the operational incident-handling capability includes containment.
[f] the operational incident-handling capability includes recovery.
[g] the operational incident-handling capability includes user response activities.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must build and maintain an incident response program covering preparation, detection, analysis, containment, recovery, and user communication. Evidence may include incident response policies, team assignments, and after-action reports. Pitfalls include lacking formal playbooks, failing to rehearse response procedures, or relying solely on ad hoc actions.

[Click here to type your detailed process]

3.5.2. Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

Assessment Objective:

Determine if:
[a] incidents are tracked.
[b] incidents are documented.
[c] authorities to whom incidents are to be reported are identified.
[d] organizational officials to whom incidents are to be reported are identified.
[e] identified authorities are notified of incidents.
[f] identified organizational officials are notified of incidents.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must ensure all incidents are tracked, documented, and reported promptly to the proper internal and external stakeholders. Evidence may include incident tracking tickets, notification logs, and regulator submission records. Pitfalls include inconsistent classification of incidents, failure to notify regulators when required, or incomplete documentation of incident details.

[Click here to type your detailed process]

3.5.3. Test the organizational incident response capability.

Assessment Objective:

Determine if the incident response capability is tested.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must regularly test their incident response procedures using exercises such as tabletop scenarios, simulations, or live-fire drills. Evidence may include exercise plans, participation records, test reports, and after-action reviews documenting lessons learned. Pitfalls include conducting tests too infrequently, failing to address findings from exercises, or excluding critical staff from participation.

[Click here to type your detailed process]

3.6. Family: Maintenance (MA)

3.6.1. Perform maintenance on organizational systems.

Assessment Objective:

Determine if system maintenance is performed.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must ensure all system maintenance is planned, documented, and executed securely by authorized personnel. Evidence may include maintenance logs, vendor service records, and approval forms for scheduled tasks. Pitfalls include failing to track unscheduled maintenance, using unauthorized staff, or not documenting changes made during maintenance.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] tools used to conduct system maintenance are controlled.
[b] techniques used to conduct system maintenance are controlled.
[c] mechanisms used to conduct system maintenance are controlled.
[d] personnel used to conduct system maintenance are controlled.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must restrict maintenance tools, techniques, and personnel to those that are authorized and secure. Evidence may include approved tool lists, personnel authorization records, and monitoring of maintenance activities. Pitfalls include allowing uncontrolled remote tools, failing to validate vendor staff, or not auditing tool usage.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must sanitize or remove Controlled Unclassified Information (CUI) from systems before sending them for off-site maintenance. Evidence may include sanitization procedures, chain-of-custody forms, and certificates of media sanitization. Pitfalls include sending devices to vendors without wiping data or failing to document sanitization steps.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must scan diagnostic and test media for malware before connecting them to systems. Evidence may include antivirus scan logs, approved test tool lists, and documented pre-use checks. Pitfalls include skipping scans for vendor-provided media or relying on outdated antivirus signatures.

[Click here to type your detailed process]

3.6.5. Require multifactor authentication to establish nonlocal maintenance sessions via external network connections.

Assessment Objective:

Determine if:
[a] multifactor authentication is used to establish nonlocal maintenance sessions via external network connections.
[b] nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must enforce multifactor authentication (MFA) for all remote maintenance sessions. Evidence may include VPN configuration policies, MFA enrollment logs, and session initiation records. Pitfalls include relying only on single-factor authentication, exempting privileged accounts, or failing to enforce MFA for vendor access.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if maintenance personnel without required access authorization are supervised during maintenance activities.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must ensure that unescorted or unauthorized personnel performing maintenance are directly supervised by authorized staff. Evidence may include visitor logs, supervision checklists, and signed oversight forms. Pitfalls include leaving vendor staff unsupervised, failing to log oversight activities, or assuming remote monitoring is sufficient for physical supervision.

[Click here to type your detailed process]

3.7. Family 3.8: Media Protection (MP)

3.7.1. Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

Assessment Objective:

Determine if:
[a] paper media containing CUI is physically controlled.
[b] digital media containing CUI is physically controlled.
[c] paper media containing CUI is securely stored.
[d] digital media containing CUI is securely stored.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must physically secure and control all media containing CUI, including both paper and digital forms. Evidence may include locked storage logs, badge-controlled access records, and encryption for digital media at rest. Pitfalls include unsecured filing cabinets, untracked removable drives, or improper disposal of paper documents.

[Click here to type your detailed process]

3.7.2. Limit access to CUI on system media to authorized users.

Assessment Objective:

Determine if access to CUI on system media is limited to authorized users.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must ensure that only explicitly authorized users can access CUI stored on any type of media. Evidence may include access control lists, role-based access permissions, and audit logs of media usage. Pitfalls include granting access by default, neglecting periodic access reviews, or not revoking permissions when users change roles.

[Click here to type your detailed process]

3.7.3. Sanitize or destroy system media containing CUI before disposal or release for reuse.

Assessment Objectives

Determine if:
[a] system media containing CUI is sanitized or destroyed before disposal.
[b] system media containing CUI is sanitized before it is released for reuse.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must sanitize or destroy CUI-bearing media before reuse or disposal, using approved methods (e.g., DoD 5220.22-M, NIST 800-88). Evidence may include sanitization logs, destruction certificates, and chain-of-custody forms. Pitfalls include relying on simple deletion, using unapproved methods, or outsourcing destruction without oversight.

[Click here to type your detailed process]

3.7.4. Mark system media containing CUI indicating distribution limitations, handling caveats, and applicable security markings (if any).

Assessment Objective:

Determine if:
[a] media containing CUI is marked with applicable CUI markings.
[b] media containing CUI is marked with distribution limitations.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must ensure that all CUI-bearing media is clearly labeled with handling caveats, security markings, and distribution limitations. Evidence may include labeling policies, examples of marked media, and audit checks of stored items. Pitfalls include inconsistent markings, missing labels on removable media, or relying only on user memory to enforce markings.

[Click here to type your detailed process]

3.7.5. Control access to system media containing CUI and maintain accountability for media during transport outside of controlled areas.

Assessment Objective:

Determine if:
[a] access to media containing CUI is controlled.
[b] accountability for media containing CUI is maintained during transport outside of controlled areas.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must enforce strict accountability when transporting CUI media outside secured facilities. Evidence may include transport logs, courier tracking receipts, and chain-of-custody forms. Pitfalls include failing to log transfers, using unsecured carriers, or neglecting to track temporary custody.

[Click here to type your detailed process]

3.7.6. Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

Assessment Objective:

Determine if the confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must encrypt CUI on digital media during transport or ensure equivalent physical safeguards. Evidence may include encryption tool logs, transport encryption policies, and keys/certificates management documentation. Pitfalls include transporting unencrypted drives, failing to protect encryption keys, or relying solely on verbal assurances from carriers.

[Click here to type your detailed process]

3.7.7. Control the use of removable media on system components.

Assessment Objective:

Determine if the use of removable media on system components is controlled.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must implement policies and technical controls restricting removable media usage to prevent unauthorized CUI transfer. Evidence may include endpoint management configurations, removable media policies, and audit logs of device connections. Pitfalls include allowing uncontrolled USB usage, failing to enforce encryption, or not monitoring removable device activity.

[Click here to type your detailed process]

3.7.8. Prohibit the use of portable storage devices when such devices have no identifiable owner.

Assessment Objective:

Determine if the use of portable storage devices is prohibited when such devices have no identifiable owner.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must restrict the use of portable storage devices unless ownership can be verified and tracked. Evidence may include asset management records, device registration logs, and policy documents prohibiting unidentified devices. Pitfalls include allowing anonymous USB drives, failing to validate device ownership, or exceptions made without risk assessment.

[Click here to type your detailed process]

3.7.9. Protect the confidentiality of backup CUI at storage locations.

Assessment Objective:

Determine if the confidentiality of backup CUI is protected at storage locations.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must secure backups containing CUI through encryption and controlled access at both on-site and off-site storage locations. Evidence may include backup encryption configurations, storage facility access logs, and periodic audit results. Pitfalls include leaving backups unencrypted, failing to protect physical access, or not rotating encryption keys.

[Click here to type your detailed process]

3.8. Family: Personnel Security (PS)

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

Assessment Objective:

Determine if individuals are screened prior to authorizing access to organizational systems containing CUI.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must perform background checks or equivalent screening before granting access to CUI systems. Evidence may include HR background check records, personnel screening policies, and signed nondisclosure agreements. Pitfalls include inconsistent application of screening standards or failing to rescreen after long employment gaps.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] a policy and/or process for terminating system access and any credentials coincident with personnel actions is established.
[b] system access and credentials are terminated consistent with personnel actions such as termination or transfer.
[c] the system is protected during and after personnel transfer actions.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must revoke or adjust access promptly when employees are terminated or transferred. Evidence may include offboarding checklists, system access revocation logs, and asset return forms. Pitfalls include delays in disabling accounts, leaving orphaned credentials active, or not updating permissions after role changes.

[Click here to type your detailed process]

3.9. Family 3.10: Physical Protection (PE)

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

Assessment Objective:

Determine if:
[a] authorized individuals allowed physical access are identified.
[b] physical access to organizational systems is limited to authorized individuals.
[c] physical access to equipment is limited to authorized individuals.
[d] physical access to operating environments is limited to authorized individuals.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must restrict physical access to servers, workstations, and facilities containing CUI to authorized staff only. Evidence may include badge access records, visitor logs, and facility access policies. Pitfalls include unsecured server rooms, propped-open doors, or failing to update access lists after personnel changes.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] the physical facility where organizational systems reside is protected.
[b] the support infrastructure for organizational systems is protected.
[c] the physical facility where organizational systems reside is monitored.
[d] the support infrastructure for organizational systems is monitored.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must secure and monitor facilities where systems are housed, including HVAC, power, and environmental controls. Evidence may include surveillance camera logs, environmental monitoring reports, and security guard logs. Pitfalls include failing to maintain monitoring equipment, ignoring environmental alerts, or inadequate surveillance coverage.

[Click here to type your detailed process]

3.9.3. Escort visitors and monitor visitor activity.

Assessment Objective:

Determine if:
[a] visitors are escorted.
[b] visitor activity is monitored.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must require escorts for visitors in controlled areas and log their activities. Evidence may include visitor access logs, escort assignment records, and video surveillance footage. Pitfalls include failing to log visits, not verifying escort presence, or leaving visitors unsupervised in secure spaces.

[Click here to type your detailed process]

3.9.4. Maintain audit logs of physical access.

Assessment Objective:

Determine if audit logs of physical access are maintained.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must record and retain logs of all physical access to secure facilities and equipment. Evidence may include electronic badge reader logs, visitor sign-in sheets, and surveillance system records. Pitfalls include failing to retain logs for the required period, incomplete visitor records, or not reviewing logs regularly.

[Click here to type your detailed process]

3.9.5. Control and manage physical access devices.

Assessment Objective:

Determine if:
[a] physical access devices are identified.
[b] physical access devices are controlled.
[c] physical access devices are managed.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must manage keys, badges, and other access devices to ensure only authorized personnel have them. Evidence may include access device issuance logs, key control policies, and inventory records. Pitfalls include failing to recover badges after termination, not tracking duplicate keys, or weak processes for temporary access.

[Click here to type your detailed process]

3.9.6. Enforce safeguarding measures for CUI at alternate work sites.

Assessment Objective:

Determine if:
[a] safeguarding measures for CUI are defined for alternate work sites.
[b] safeguarding measures for CUI are enforced for alternate work sites.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must ensure staff follow security protocols when handling CUI outside primary facilities, such as remote or alternate worksites. Evidence may include telework security policies, VPN usage reports, and employee attestations of compliance. Pitfalls include unsecured home offices, use of personal devices without safeguards, or neglecting to monitor compliance.

[Click here to type your detailed process]

3.10. Family 3.11: Risk Assessment (RA)

3.10.1. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

Assessment Objective:

Determine if:
[a] the frequency to assess risk to organizational operations, organizational assets, and individuals is defined.
[b] risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must conduct recurring risk assessments to evaluate threats and vulnerabilities to systems processing CUI. Evidence may include risk assessment reports, risk registers, and meeting notes documenting mitigation strategies. Pitfalls include infrequent assessments, ignoring business impact, or failing to reassess after major system changes.

[Click here to type your detailed process]

3.10.2. Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

Assessment Objective:

Determine if:
[a] the frequency to scan for vulnerabilities in organizational systems and applications is defined.
[b] vulnerability scans are performed on organizational systems with the defined frequency.

[c] vulnerability scans are performed on applications with the defined frequency.
[d] vulnerability scans are performed on organizational systems when new vulnerabilities are identified.
[e] vulnerability scans are performed on applications when new vulnerabilities are identified.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must perform vulnerability scans on systems and applications regularly and in response to new threats. Evidence may include vulnerability scan results, remediation tickets, and scanning tool configurations. Pitfalls include scanning only annually, failing to act on scan findings, or excluding critical systems from scans.

[Click here to type your detailed process]

3.10.3. Remediate vulnerabilities in organizational systems and applications in accordance with risk assessments.

Assessment Objective:

Determine if:
[a] vulnerabilities are identified.
[b] vulnerabilities are remediated in accordance with risk assessments.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must remediate identified vulnerabilities in line with their risk assessment priorities. Evidence may include remediation plans, patch deployment logs, and vulnerability management dashboards. Pitfalls include leaving high-risk vulnerabilities unresolved, prioritizing convenience over risk, or failing to track remediation progress.

[Click here to type your detailed process]

3.11. Family: Security Assessment (CA)

3.11.1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

Assessment Objective:

Determine if:
[a] the frequency of security control assessments is defined.
[b] security controls are assessed with the defined frequency to determine if the controls are effective in their application.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must conduct periodic security control assessments to confirm effectiveness in protecting CUI. Evidence may include assessment reports, POA&Ms (Plans of Action and Milestones), and assessor evaluation records. Pitfalls include assessments done too infrequently, incomplete scope, or ignoring assessor findings.

[Click here to type your detailed process]

3.11.2. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

Assessment Objective:

Determine if:
[a] deficiencies and vulnerabilities to be addressed by the plan of action are identified.
[b] a plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities.
[c] the plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must document and carry out remediation activities through formal plans of action. Evidence may include POA&Ms, remediation tracking logs, and updated security policies. Pitfalls include creating plans but not implementing them, failing to prioritize by risk, or leaving deficiencies open indefinitely.

[Click here to type your detailed process]

3.11.3. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Assessment Objective:

Determine if security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must continuously monitor security controls, leveraging tools and processes to validate ongoing effectiveness. Evidence may include automated monitoring dashboards, continuous assessment logs, and periodic audit records. Pitfalls include treating monitoring as a one-time event, ignoring alerts, or failing to document ongoing review results.

[Click here to type your detailed process]

3.11.4. Develop, document, and periodically update system security plans that describe system boundaries, operational environment, how security requirements are implemented, and the relationships with or connections to other systems.

Assessment Objective:

Determine if:
[a] a system security plan is developed.
[b] the system boundary is described and documented in the system security plan.
[c] the system environment of operation is described and documented in the system security plan.
[d] the security requirements identified and approved by the designated authority as non-applicable are identified.
[e] the method of security requirement implementation is described and documented in the system security plan.
[f] the relationship with or connection to other systems is described and documented in the system security plan.
[g] the frequency to update the system security plan is defined.
[h] system security plan is updated with the defined frequency.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must maintain comprehensive system security plans (SSPs) that define system boundaries, environments, security implementations, and interconnections. Evidence may include SSP documents, SSP update logs, and architecture diagrams. Pitfalls include outdated SSPs, incomplete descriptions of system boundaries, or failing to update plans after major changes.

[Click here to type your detailed process]

3.12. Family: System and Communications Protection (SC)

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

Assessment Objective:

Determine if:
[a] the external system boundary is defined.
[b] key internal system boundaries are defined.
[c] communications are monitored at the external system boundary.
[d] communications are monitored at key internal boundaries.
[e] communications are controlled at the external system boundary.
[f] communications are controlled at key internal boundaries.
[g] communications are protected at the external system boundary.
[h] communications are protected at key internal boundaries.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must secure communications at both external and critical internal boundaries using monitoring, filtering, and protective technologies. Evidence may include firewall configurations, intrusion detection system (IDS) logs, and network diagrams. Pitfalls include failing to monitor internal segments, inconsistent firewall rules, or relying only on perimeter defenses.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] architectural designs that promote effective information security are identified.
[b] software development techniques that promote effective information security are identified.
[c] systems engineering principles that promote effective information security are identified.
[d] identified architectural designs that promote effective information security are employed.
[e] identified software development techniques that promote effective information security are employed.
[f] identified systems engineering principles that promote effective information security are employed.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must incorporate security into system architecture and software development from the outset. Evidence may include secure design documents, coding standards, and threat modeling outputs. Pitfalls include retrofitting security late in the lifecycle, neglecting secure coding practices, or failing to align architecture with security principles.

[Click here to type your detailed process]

3.12.3. Separate user functionality from system management functionality.

Assessment Objective:

Determine if:
[a] user functionality is identified.
[b] system management functionality is identified.
[c] user functionality is separated from system management functionality.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must ensure that standard users cannot access system management functions. Evidence may include access control configurations, privilege separation documentation, and account role assignments. Pitfalls include combining user and admin roles, shared credentials, or failing to enforce separation in application interfaces.

[Click here to type your detailed process]

3.12.4. Prevent unauthorized and unintended information transfer via shared system resources.

Assessment Objective:

Determine if unauthorized and unintended information transfer via shared system resources is prevented.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must protect against information leakage through shared resources such as memory, storage, or networking components. Evidence may include virtualization isolation settings, configuration baselines, and penetration test results. Pitfalls include weak multi-tenant controls, failing to separate virtual machines properly, or not monitoring shared resource use.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] publicly accessible system components are identified.

[b] subnetworks for publicly accessible system components are physically or logically separated from internal networks.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must isolate publicly accessible systems (e.g., web servers) from internal networks using DMZs or segmentation. Evidence may include network architecture diagrams, firewall rules, and VLAN configurations. Pitfalls include placing public-facing servers directly on internal networks, poor segmentation enforcement, or not monitoring DMZ activity.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] network communications traffic is denied by default.
[b] network communications traffic is allowed by exception.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must configure firewalls and routers to block all network traffic by default, allowing only explicitly authorized communications. Evidence may include firewall configuration baselines, change approval records, and network monitoring logs. Pitfalls include using overly permissive firewall rules, failing to review exceptions, or leaving unused ports open.

[Click here to type your detailed process]

3.12.7. Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating through external networks (i.e., split tunneling).

Assessment Objective:

Determine if remote devices are prevented from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks (i.e., split tunneling).

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must disable split tunneling to ensure remote devices route all traffic through secure organizational channels. Evidence may include VPN client configurations, endpoint security settings, and remote access policy documents. Pitfalls include leaving split tunneling enabled, not verifying vendor device configurations, or failing to enforce policies across all users.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified.
[b] alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified.
[c] either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must protect CUI in transit by using strong encryption protocols (e.g., TLS 1.2+, IPsec, SSH). Evidence may include configuration screenshots, key management policies, and penetration test results confirming secure transmission. Pitfalls include using outdated protocols like SSLv3/TLS 1.0, weak ciphers, or failing to rotate encryption keys.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] a period of inactivity to terminate network connections associated with communications sessions is defined.
[b] network connections associated with communications sessions are terminated at the end of the sessions.
[c] network connections associated with communications sessions are terminated after the defined period of inactivity.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must configure systems to automatically terminate network connections after sessions end or following a period of inactivity. Evidence may include system timeout configurations, firewall session logs, and screenshots of VPN/remote access settings. Pitfalls include overly long inactivity periods, failing to apply policies to privileged sessions, or leaving stale connections open.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] cryptographic keys are established whenever cryptography is employed.
[b] cryptographic keys are managed whenever cryptography is employed.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must implement secure processes for key generation, distribution, rotation, and destruction. Evidence may include key management policies, hardware security module (HSM) records, and logs of key lifecycle events. Pitfalls include storing keys in plaintext, reusing weak keys, or neglecting timely key rotation.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if FIPS-validated cryptography is employed to protect the confidentiality of CUI.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must use only FIPS 140-validated cryptographic modules to protect CUI confidentiality. Evidence may include system encryption settings, cryptographic module validation certificates, and vendor documentation.

Pitfalls include using non-validated algorithms, misconfigured crypto libraries, or failing to enforce FIPS mode across all systems.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] collaborative computing devices are identified.
[b] collaborative computing devices provide indication to users of devices in use.
[c] remote activation of collaborative computing devices is prohibited.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must prevent remote activation of microphones, cameras, and similar devices without user awareness, and provide visible/audible indicators when devices are in use. Evidence may include collaboration tool policies, device configuration settings, and system security test results. Pitfalls include enabling remote activation by default, failing to configure indicators, or not training users to recognize device status.

[Click here to type your detailed process]

3.12.13. Control and monitor the use of mobile code.

Assessment Objective:

Determine if:
[a] use of mobile code is controlled.
[b] use of mobile code is monitored.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must establish and enforce policies for controlling and monitoring mobile code such as Java, JavaScript, or ActiveX. Evidence may include secure configuration baselines, monitoring logs, and policy documents. Pitfalls include leaving mobile code unrestricted, failing to update controls for new mobile code types, or ignoring alerts related to malicious code.

[Click here to type your detailed process]

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

Assessment Objective:

Determine if:
[a] use of Voice over Internet Protocol (VoIP) technologies is controlled.
[b] use of Voice over Internet Protocol (VoIP) technologies is monitored.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must secure and monitor VoIP technologies to prevent interception or misuse. Evidence may include VoIP security policies, call monitoring records, and firewall/IDS configurations. Pitfalls include using unsecured VoIP protocols, failing to encrypt VoIP traffic, or not monitoring call activity for anomalies.

[Click here to type your detailed process]

3.12.15.Protect the authenticity of communications sessions.

Assessment Objective:

Determine if the authenticity of communications sessions is protected.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must safeguard communication sessions against impersonation or tampering using strong authentication and integrity controls. Evidence may include TLS certificates, digital signatures, and session logs. Pitfalls include expired certificates, weak integrity algorithms, or not validating digital signatures.

[Click here to type your detailed process]

3.12.16. Protect the confidentiality of CUI at rest.

Assessment Objective:

Determine if the confidentiality of CUI at rest is protected.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must ensure that CUI stored on systems is encrypted using FIPS-validated cryptographic methods. Evidence may include encryption configurations, data-at-rest policies, and audit logs verifying encryption enforcement. Pitfalls include storing CUI on unencrypted drives, failing to rotate encryption keys, or mismanaging cryptographic modules.

[Click here to type your detailed process]

3.13. Family: System and Information Integrity (SI)

3.13.1. Identify, report, and correct system flaws in a timely manner.

Assessment Objective:

Determine if:
[a] the time within which to identify system flaws is specified.
[b] system flaws are identified within the specified time frame.
[c] the time within which to report system flaws is specified.
[d] system flaws are reported within the specified time frame.
[e] the time within which to correct system flaws is specified.
[f] system flaws are corrected within the specified time frame.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must establish processes to detect, report, and remediate system flaws quickly. Evidence may include vulnerability management tickets, patch logs, and timelines of remediation activities. Pitfalls include delayed patching, incomplete flaw reporting, or ignoring vendor advisories.

[Click here to type your detailed process]

3.13.2. Provide protection from malicious code at appropriate locations within organizational systems.

Assessment Objective:

Determine if:
[a] designated locations for malicious code protection are identified.
[b] protection from malicious code at designated locations is provided.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must deploy anti-malware solutions at key entry points such as endpoints, servers, and email gateways. Evidence may include antivirus deployment reports, EDR logs, and policy documents. Pitfalls include relying on outdated tools, not updating signatures, or failing to monitor alert activity.

[Click here to type your detailed process]

3.13.3. Monitor system security alerts and advisories and take action in response.

Assessment Objective:

Determine if:
[a] response actions to system security alerts and advisories are identified.
[b] system security alerts and advisories are monitored.
[c] actions in response to system security alerts and advisories are taken.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must monitor sources of security advisories and act on relevant alerts. Evidence may include subscription records for alerts (e.g., US-CERT), incident response logs, and patch implementation reports. Pitfalls include ignoring advisories, lack of defined responsibility for monitoring, or failure to prioritize responses.

[Click here to type your detailed process]

3.13.4. Update malicious code protection mechanisms when new releases are available.

Assessment Objective:

Determine if malicious code protection mechanisms are updated when new releases are available.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must keep anti-malware tools current by promptly applying signature and engine updates. Evidence may include update logs, EDR dashboards, and automated patching schedules. Pitfalls include missed updates due to misconfigured systems, relying on manual updates, or failing to verify deployment across all devices.

[Click here to type your detailed process]

3.13.5. Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

Assessment Objective:

Determine if:
[a] the frequency for malicious code scans is defined.
[b] malicious code scans are performed with the defined frequency.
[c] real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must implement both scheduled and real-time scans to detect malicious code and vulnerabilities. Evidence may include antivirus scan reports, EDR agent dashboards, and scheduling policies. Pitfalls include disabling real-time scanning for performance reasons, inconsistent scan schedules, or failing to scan external media.

[Click here to type your detailed process]

3.13.6. Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

Assessment Objective:

Determine if:
[a] the system is monitored to detect attacks and indicators of potential attacks.
[b] inbound communications traffic is monitored to detect attacks and indicators of potential attacks.
[c] outbound communications traffic is monitored to detect attacks and indicators of potential attacks.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must deploy monitoring tools to detect suspicious activity in both inbound and outbound traffic. Evidence may include IDS/IPS logs, SOC monitoring reports, and alert response procedures. Pitfalls include monitoring only inbound traffic, not correlating logs from multiple sources, or ignoring outbound anomalies that may indicate compromise.

[Click here to type your detailed process]

3.13.7. Identify unauthorized use of organizational systems.

Assessment Objective:

Determine if:
[a] authorized use of the system is defined.
[b] unauthorized use of the system is identified.

Status: □ Implemented □ Planned □ Not Applicable

Strike Graph Guidance: Organizations must detect and respond to unauthorized system use through auditing and monitoring. Evidence may include audit logs, anomalous user activity reports, and incident investigation records. Pitfalls include not defining what constitutes unauthorized use, failing to monitor for privilege misuse, or not alerting on suspicious activity.

[Click here to type your detailed process]