

secureframe

CMMC SSP

System Security Plan

Prepared for:

Last updated:

1. System Identification

1.1. System Name/Title:

System Categorization: Impact for Confidentiality

1.1.1. 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:	

1.2.1.1. System Owner (assignment of security responsibility):

Name:	
Title:	
Office Address:	
Work Phone:	
e-Mail Address:	

1.2.1.2. 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? What does your company do? What services do you provide?

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?

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. Access Control

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[f] system access is limited to authorized devices (including other systems).

Example: {Company name} enforces system access based on the concept of least privilege. Users only have access to systems and vendors for which they need. Application, system, and database administrator privileges are limited to members of the engineering, compliance, customer success, and security teams as needed. System access and privileges are provisioned and granted through {system/tool name}.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] the types of transactions and functions that authorized users are permitted to execute are defined; and

[b] system access is limited to the defined types of transactions and functions for authorized users.

Example: Administrative access to production servers and databases is restricted based on the principle of least privilege to management and engineers who have a job function and business need for such access.

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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[e] approved authorizations for controlling the flow of CUI are enforced.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] the duties of individuals requiring separation are defined;

[b] responsibilities for duties that require separation are assigned to separate individuals; and

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

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[d] access to security functions is authorized in accordance with the principle of least privilege.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] nonsecurity functions are identified; and

[b] users are required to use non-privileged accounts or roles when accessing nonsecurity functions.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] privileged functions are defined;

[b] non-privileged users are defined;

[c] non-privileged users are prevented from executing privileged functions; and

▪
[d] the execution of privileged functions is captured in audit logs.

3.1.8. Limit unsuccessful login attempts.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked “Not Applicable.”

Assessment objectives

Determine if:

*[a] the means of limiting unsuccessful logon attempts is defined; and
[b] the defined means of limiting unsuccessful logon attempts is implemented.*

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked “Not Applicable.”

Assessment objectives

Determine if:

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

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and
[c] previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.*

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] conditions requiring a user session to terminate are defined; and

[b] a user session is automatically terminated after any of the defined conditions occur.

3.1.12. Monitor and control remote access sessions.

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] remote access sessions are permitted;

[b] the types of permitted remote access are identified;

[c] remote access sessions are controlled; and

[d] remote access sessions are monitored.

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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] cryptographic mechanisms to protect the confidentiality of remote access sessions are identified; and

[b] cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.



3.1.14. Route remote access via managed access control points.

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

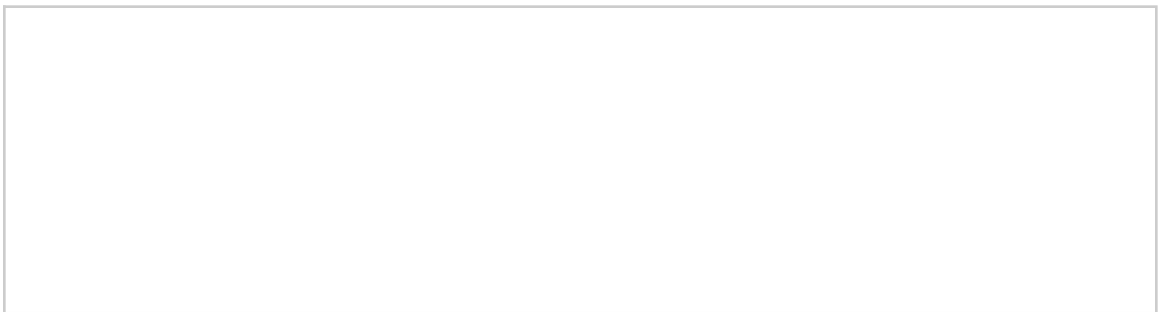
Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] managed access control points are identified and implemented; and

[b] remote access is routed through managed network access control points.



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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked “Not Applicable.”

Assessment objectives

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; and
- [d] access to the identified security-relevant information via remote access is authorized.

3.1.16. Authorize wireless access prior to allowing such connections.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked “Not Applicable.”

Assessment objectives

Determine if:

- [a] wireless access points are identified; and
- [b] wireless access is authorized prior to allowing such connections.

3.1.17. Protect wireless access using authentication and encryption.

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] wireless access to the system is protected using authentication; and

[b] wireless access to the system is protected using encryption.

3.1.18. Control connection of mobile devices.

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] mobile devices that process, store, or transmit CUI are identified;

[b] mobile device connections are authorized; and

[c] mobile device connections are monitored and logged.

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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] mobile devices and mobile computing platforms that process, store, or transmit CUI are identified; and

[b] encryption is employed to protect CUI on identified mobile devices and mobile computing platforms.

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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[f] the use of external systems is controlled/limited.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[c] the use of portable storage devices containing CUI on external systems is limited as defined.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and*
- [e] mechanisms are in place to remove and address improper posting of CUI.*

3.2. Awareness and Training

3.2.1. Ensure that managers, systems 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.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and*
- [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.*

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and
[c] personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.*

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

▪

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

3.3. Audit and Accountability

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[f] audit records are retained as defined.

- 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.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] the content of the audit records needed to support the ability to uniquely trace users to their actions is defined; and

[b] audit records, once created, contain the defined content.

- 3.3.3. Review and update logged events.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[c] event types being logged are updated based on the review.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[c] identified personnel or roles are alerted in the event of an audit logging process failure.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[b] defined audit record review, analysis, and reporting processes are correlated.

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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] an audit record reduction capability that supports on-demand analysis is provided; and

[b] a report generation capability that supports on-demand reporting is provided.

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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and
- [c] internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and
- [f] audit logging tools are protected from unauthorized deletion.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] a subset of privileged users granted access to manage audit logging functionality is defined; and

[b] management of audit logging functionality is limited to the defined subset of privileged users.

3.4. Configuration Management

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] a baseline configuration is established;

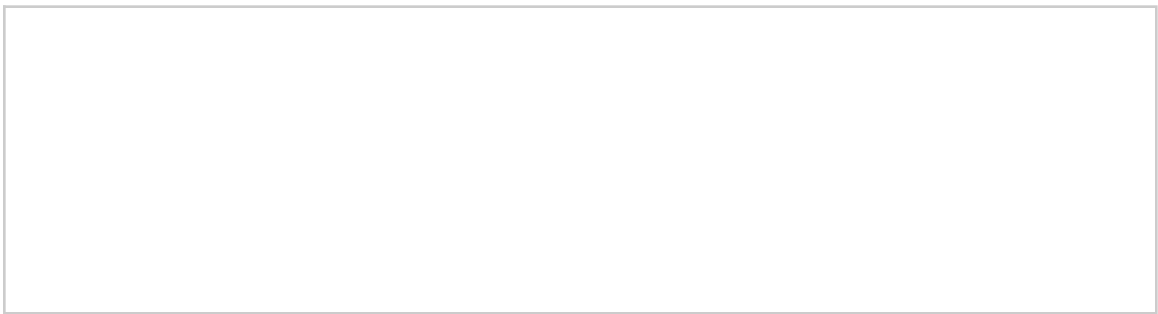
[b] the baseline configuration includes hardware, software, firmware, and documentation;

[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; and

[f] the inventory is maintained (reviewed and updated) throughout the system development life cycle.



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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] security configuration settings for information technology products employed in the system are established and included in the baseline configuration; and

[b] security configuration settings for information technology products employed in the system are enforced.

3.4.3. Track, review, approve or disapprove, and log changes to organizational systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[d] changes to the system are logged.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] the security impact of changes to the system is analyzed prior to implementation.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked “Not Applicable.”

Assessment objectives

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;

[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;
and*

[h] logical access restrictions associated with changes to the system are enforced.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked “Not Applicable.”

Assessment objectives

Determine if:

[a] essential system capabilities are defined based on the principle of least functionality; and

[b] the system is configured to provide only the defined essential capabilities.

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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked “Not Applicable.”

Assessment objectives

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; and

[o] the use of nonessential services is restricted, disabled, or prevented as defined.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[c] whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified.

- 3.4.9. Control and monitor user-installed software.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[c] installation of software by users is monitored.

3.5. Identification and Authentication

3.5.1. Identify system users, processes acting on behalf of users, and devices.

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] system users are identified;

[b] processes acting on behalf of users are identified; and

[c] devices accessing the system are identified.

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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[c] the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.

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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[d] multifactor authentication is implemented for network access to non-privileged accounts.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] replay-resistant authentication mechanisms are implemented for network account access to privileged and non-privileged accounts.

3.5.5. Prevent reuse of identifiers for a defined period.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

*[a] a period within which identifiers cannot be reused is defined; and
[b] reuse of identifiers is prevented within the defined period.*

3.5.6. Disable identifiers after a defined period of inactivity.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

*[a] a period of inactivity after which an identifier is disabled is defined; and
[b] identifiers are disabled after the defined period of inactivity.*

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and*

▪
[d] minimum password change of character requirements as defined are enforced when new passwords are created.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] the number of generations during which a password cannot be reused is specified and

[b] reuse of passwords is prohibited during the specified number of generations.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

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

3.5.10. Store and transmit only cryptographically-protected passwords.

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] passwords are cryptographically protected in storage; and

[b] passwords are cryptographically protected in transit.

3.5.11. Obscure feedback of authentication information.

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

▪
[a] authentication information is obscured during the authentication process.

3.6. Incident Response

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and*
- [g] the operational incident-handling capability includes user response activities.*

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[f] identified organizational officials are notified of incidents.

- 3.6.3. Test the organizational incident response capability

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] the incident response capability is tested.

3.7. Maintenance

3.7.1. Perform maintenance on organizational systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] system maintenance is performed.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

▪
[d] personnel used to conduct system maintenance are controlled.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] equipment to be removed from organizational spaces for off-site maintenance is sanitized of any CUI.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

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

- 3.7.5. Require multi-factor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

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

- 3.7.6. Supervise the maintenance activities of maintenance personnel without required access authorization.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] maintenance personnel without required access authorization are supervised during maintenance activities.

3.8. Media Protection

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[d] digital media containing CUI is securely stored.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked “Not Applicable.”

Assessment objectives

Determine if:

[a] access to CUI on system media is limited to authorized users.

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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked “Not Applicable.”

Assessment objectives

Determine if:

[a] system media containing CUI is sanitized or destroyed before disposal; and

[b] system media containing CUI is sanitized before it is released for reuse.

3.8.4. Mark media with necessary CUI markings and distribution limitations.

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked “Not Applicable.”

▪

Assessment objectives

Determine if:

[a] media containing CUI is marked with applicable CUI markings; and

[b] media containing CUI is marked with distribution limitations.

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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] access to media containing CUI is controlled; and

[b] accountability for media containing CUI is maintained during transport outside of controlled areas.

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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked “Not Applicable.”

Assessment objectives

Determine if:

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

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked “Not Applicable.”

Assessment objectives

Determine if:

[a] the use of removable media on system components is controlled.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked “Not Applicable.”

▪

Assessment objectives

Determine if:

[a] the use of portable storage devices is prohibited when such devices have no identifiable owner.

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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] the confidentiality of backup CUI is protected at storage locations.

3.9. Personnel Security

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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

■

Assessment objectives

Determine if:

[a] individuals are screened prior to authorizing access to organizational systems containing CUI.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[c] the system is protected during and after personnel transfer actions.

3.10. Physical Protection

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and*
- [d] physical access to operating environments is limited to authorized individuals.*

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and*
- [d] the support infrastructure for organizational systems is monitored.*

3.10.3. Escort visitors and monitor visitor activity.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] visitors are escorted; and

[b] visitor activity is monitored.

3.10.4. Maintain audit logs of physical access.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] audit logs of physical access are maintained.

3.10.5. Control and manage physical access devices.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

- [a] physical access devices are identified;*
- [b] physical access devices are controlled; and*
- [c] physical access devices are managed.*

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

- [a] safeguarding measures for CUI are defined for alternate work sites; and*
- [b] safeguarding measures for CUI are enforced for alternate work sites.*

3.11. Risk Assessment

3.11.1. 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.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] the frequency to assess risk to organizational operations, organizational assets, and individuals is defined; and

[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.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[e] vulnerability scans are performed on applications when new vulnerabilities are identified.

3.11.3. Remediate vulnerabilities in accordance with risk assessments.

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] vulnerabilities are identified; and

[b] vulnerabilities are remediated in accordance with risk assessments.

3.12. Security Assessment

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] the frequency of security control assessments is defined; and

[b] security controls are assessed with the defined frequency to determine if the controls are effective in their application.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and
[c] the plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] security controls are monitored on an ongoing basis to ensure the continued effectiveness of those controls.

3.12.4. Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked “Not Applicable.”

Assessment objectives

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; and
- [h] system security plan is updated with the defined frequency.

3.13. System and Communications Protection

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked “Not Applicable.”

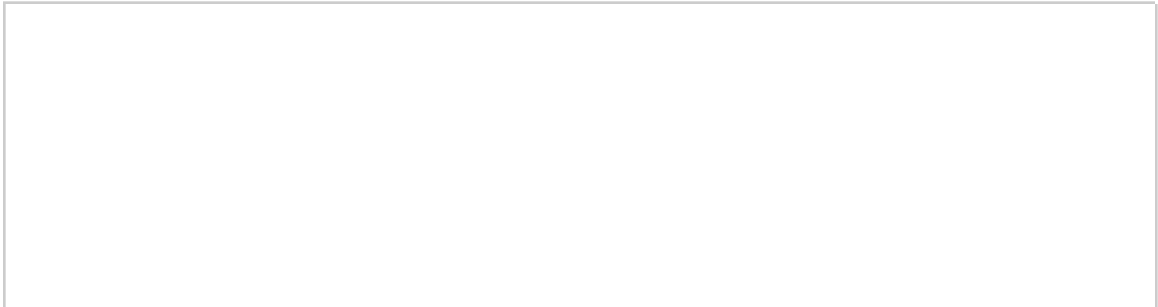
Assessment objectives

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; and
[h] communications are protected at key internal boundaries.*



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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and
[f] identified systems engineering principles that promote effective information security are employed.*

3.13.3. Separate user functionality from system management functionality.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] user functionality is identified;

[b] system management functionality is identified; and

[c] user functionality is separated from system management functionality.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] unauthorized and unintended information transfer via shared system resources is prevented.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] publicly accessible system components are identified; and

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

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] network communications traffic is denied by default; and

[b] network communications traffic is allowed by exception.

3.13.7. Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] 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).

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and
[c] either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and
[c] network connections associated with communications sessions are terminated after the defined period of inactivity.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

*[a] cryptographic keys are established whenever cryptography is employed; and
[b] cryptographic keys are managed whenever cryptography is employed.*

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] FIPS-validated cryptography is employed to protect the confidentiality of CUI.

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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] collaborative computing devices are identified;

[b] collaborative computing devices provide indication to users of devices in use; and

[c] remote activation of collaborative computing devices is prohibited.

3.13.13. Control and monitor the use of mobile code.

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] use of mobile code is controlled; and

[b] use of mobile code is monitored.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] use of Voice over Internet Protocol (VoIP) technologies is controlled; and

[b] use of Voice over Internet Protocol (VoIP) technologies is monitored.

3.13.15. Protect the authenticity of communications sessions.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] the authenticity of communications sessions is protected.

3.13.16. Protect the confidentiality of CUI at rest.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] the confidentiality of CUI at rest is protected.

3.14. System and Information Integrity

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

☐ Implemented

☐ Planned to be Implemented

☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[f] system flaws are corrected within the specified time frame.

3.14.2. Provide protection from malicious code at designated locations within organizational systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

*[a] designated locations for malicious code protection are identified; and
[b] protection from malicious code at designated locations is provided.*

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

*[a] response actions to system security alerts and advisories are identified;
[b] system security alerts and advisories are monitored; and
[c] actions in response to system security alerts and advisories are taken.*

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] malicious code protection mechanisms are updated when new releases are available.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] the frequency for malicious code scans is defined;

[b] malicious code scans are performed with the defined frequency; and

[c] real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.

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

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

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; and

[c] outbound communications traffic is monitored to detect attacks and indicators of potential attacks.

3.14.7. Identify unauthorized use of organizational systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Detail current implementation or planned implementation details or rationale if marked "Not Applicable."

Assessment objectives

Determine if:

[a] authorized use of the system is defined; and

[b] unauthorized use of the system is identified.

.

4. RECORD OF CHANGES

Date	Description	Made By: