2

المركـز الوطنـي للأمـن السيبرانـي
National Cyber Security Center

Critical Infrastructure Cyber Security Controls

CICSC CONTROLS

December 2024

CONTENTS

1 INTRODUCTION

The 405 customised controls included within the Critical Infrastructure Cyber Security Controls (CICSC) are derived from the following publications:

> Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations, (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication 800-53 Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5
>
> Stouffer KA, Lightman S, Pillitteri VY, Abrams M, Hahn A (2015) Guide to Industrial Control Systems (ICS) Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-82, Rev. 3. https://doi.org/10.6028/NIST.SP.800-82r3
>
> Joint Task Force (2020) Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53B. https://doi.org/10.6028/NIST.SP.800-53B

Original control text is republished courtesy of the National Institute of Standards and Technology (NIST).

Collectively, these contain a suite of security controls for information systems and operational technology that provide a comprehensive control framework for the protection of Jordan's critical infrastructure data.

Each chapter includes customised controls drawn from a NIST SP 800-53 (rev.5) Control Families to provide common guidance to operators of Jordan's critical infrastructure. At the start of each Control Family, a summary table shows the security controls included in the section and applicable Implementation Levels for each control and control enhancement.

All organisations are expected to implement Level 1 controls (135), which are designed to provide a baseline level of protection for all critical infrastructure operators. The selection and adoption of Level 2 controls (161, which provide enhanced protection) and Level 3 controls (109, which help counter more advanced threats) should be determined based on an assessment of criticality and agreed between the critical infrastructure organisation, relevant regulator, and Jordan's National Cyber Security Centre.

For information about implementing the controls see the CICSC Guidance.

See the CICSC Annex for additional information from NIST SP 800-53 (rev.5) about the context of the controls and where relevant control alignment to Jordan's National Cybersecurity Framework.

2 CONTROL FAMILY: ACCESS CONTROL

2.1 Control Implementation Levels

Control ID	**Control** | Control Enhancement	Implementation Level		
AC-1	**Policy and Procedures**	1		
AC-2	**Account Management**	1		
AC-2(1)	Automated System Account Management		2	
AC-2(2)	Automated Temporary and Emergency Account Management		2	
AC-2(3)	Disable Accounts		2	
AC-2(4)	Automated Audit Actions		2	
AC-2(5)	Inactivity Logout		2	
AC-2(9)	Restrictions on Use of Shared and Group Accounts			3
AC-2(11)	Usage Conditions			3
AC-2(12)	Account Monitoring for Atypical Usage			3
AC-2(13)	Disable Accounts for High-risk Individuals		2	
AC-3	**Access Enforcement**	1		
AC-3(11)	Restrict Access to Specific Information Types			3
AC-4	**Information Flow Enforcement**		2	
AC-4(4)	Flow Control of Encrypted Information			3
AC-5	**Separation of Duties**		2	
AC-6	**Least Privilege**		2	
AC-6(1)	Authorize Access to Security Functions		2	
AC-6(2)	Non-privileged Access for Nonsecurity Functions		2	
AC-6(3)	Network Access to Privileged Commands			3
AC-6(5)	Privileged Accounts		2	
AC-6(7)	Review of User Privileges		2	
AC-6(9)	Log Use of Privileged Functions		2	
AC-6(10)	Prohibit Non-privileged Users from Executing Privileged Functions		2	
AC-7	**Unsuccessful Logon Attempts**	1		
AC-8	**System Use Notification**	1		
AC-10	**Concurrent Session Control**			3
AC-11	**Device Lock**	1		
AC-11(1)	Pattern-hiding Displays		2	
AC-12	**Session Termination**		2	
AC-14	**Permitted Actions Without Identification or Authentication**	1		
AC-16	**Security and Privacy Attributes**			3

Control ID	**Control** | Control Enhancement	**Implementation Level**		
AC-17	**Remote Access**	1		
AC-17(1)	Monitoring and Control		2	
AC-17(2)	Protection of Confidentiality and Integrity Using Encryption		2	
AC-17(3)	Managed Access Control Points		2	
AC-17(4)	Privileged Commands and Access		2	
AC-17(9)	Disconnect or Disable Access			3
AC-17(10)	Authenticate Remote Commands			3
AC-18	**Wireless Access**	1		
AC-18(1)	Authentication and Encryption		2	
AC-18(3)	Disable Wireless Networking		2	
AC-18(4)	Restrict Configurations by Users			3
AC-18(5)	Antennas and Transmission Power Levels			3
AC-19	**Access Control for Mobile Devices**	1		
AC-19(5)	Full Device or Container-based Encryption		2	
AC-20	**Use of External Systems**	1		
AC-20(1)	Limits on Authorized Use		2	
AC-20(2)	Portable Storage Devices — Restricted Use		2	
AC-21	**Information Sharing**		2	
AC-22	**Publicly Accessible Content**	1		
AC-23	**Data Mining Protection**		2	

2.2 Controls

AC-1 Policy and Procedures

Implementation Level 1

Control a. Develop, document, and disseminate to appropriate personnel or roles:

1. An access control policy that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Is consistent with applicable laws, customer requirements, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the access control policy and the associated access controls;

b. Designate an individual to manage the development, documentation, and dissemination of the access control policy and procedures; and

c. Review and update the current access control policy:

1. Policy annually and following significant change and
2. Procedures annually and following significant change.

Considerations The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems. OT access by vendors and maintenance staff can occur over a large facility footprint or geographic area and into unobserved spaces, such as mechanical or electrical rooms, ceilings, floors, field substations, switch and valve vaults, and pump stations.

AC-2 Account Management

Implementation Level I

Control a. Define and document the types of accounts allowed and specifically prohibited for use within the system;

b. Assign account managers;

c. Require prerequisites and criteria for group and role membership;

d. Specify:

1. Authorized users of the system;
2. Group and role membership; and
3. Access authorizations (i.e. privileges) and other attributes as required for each account;

e. Require approvals by the appropriate information system owner for requests to create information accounts;

f. Create, enable, modify, disable, and remove accounts in accordance with documented policy, procedures, prerequisites, and criteria;

g. Monitor the use of accounts;

h. Notify account managers and information system owners within:

1. Defined organizational policy timeframe (e.g. 5 working days) when accounts are no longer required;
2. Defined organizational policy timeframe (e.g. 5 working days) when users are terminated or transferred; and
3. Defined organizational policy timeframe (e.g. 5 working days) when system usage or need-to-know changes for an individual;
4. Defined organizational policy timeframe (e.g. 5 working days) when service accounts are no longer needed or in-use;

i. Authorize access to the system based on:

1. A valid access authorization;
2. Intended system usage; and
3. Other attributes as required by the business functions.

j. Review accounts for compliance with account management requirements as defined in organizational policy (e.g. every 6 months);

k. Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and

l. Align account management processes with personnel termination and transfer processes.

Considerations In OT systems, physical security, personnel security, intrusion detection, or auditing measures may support this control objective.

AC-2(1) Account Management | Automated System Account Management

Implementation Level 2

Control Support the management of system accounts using automated mechanisms.

Considerations No additional OT clarification is required for this control.

AC-2(2) Account Management | Automated Temporary and Emergency Account Management

Implementation Level 2

Control Automatically disable temporary and emergency accounts as defined in organizational policy (e.g. 5 working days) of non-use.

Considerations When the OT (e.g., field devices) cannot support temporary or emergency accounts, this enhancement does not apply. Example compensating controls include employing nonautomated mechanisms or procedures.

AC-2(3) Account Management | Disable Accounts

Implementation Level 2

Control Disable accounts within defined organizational policy timeframe (e.g. 5 working days) when the accounts:

a. Have expired;

b. Are no longer associated with a user or individual;

c. Are in violation of organizational policy; or

d. Have been inactive for more than defined organizational policy (e.g. 60 calendar days).

Considerations No additional OT clarification is required for this control.

AC-2(4) Account Management | Automated Audit Actions

Implementation Level 2

Control Automatically audit account creation, modification, enabling, disabling, and removal actions.

Considerations No additional OT clarification is required for this control.

AC-2(5) Account Management | Inactivity Logout

Implementation Level 2

Control Require that users log out from their account when machines is unattended for a long period of time.

Considerations This control enhancement defines situations or timeframes in which users log out of accounts in the policy. Automatic enforcement is not addressed by this control enhancement. Organizations determine whether this control enhancement is appropriate for the mission and/or functions of the OT system and define the timeframe or scenarios. If no timeframe or scenarios apply, the organization-defined parameter reflects as much.

AC-2(9) Account Management | Restrictions on Use of Shared and Group Accounts

Implementation Level 3

Control Only permit the use of shared and group accounts that have been approved for use by the IT/OT Information System Owner and Security Authority e.g. local security contact.

Considerations No additional OT clarification is required for this control.

AC-2(11) Account Management | Usage Conditions

Implementation Level 3

Control Enforce conditional access and acceptable use policies for system or privleged accounts.

Considerations No additional OT clarification is required for this control.

AC-2(12) Account Management | Account Monitoring for Atypical Usage

Implementation Level **3**

Control (a) Monitor system accounts for multiple failed login attempts or logins from unknown locations; and

(b) Report atypical usage of system accounts to Help Desk or Information Security Team.

Considerations No additional OT clarification is required for this control.

AC-2(13) Account Management | Disable Accounts for High-risk Individuals

Implementation Level **2**

Control Disable accounts of individuals as per organizational policy (e.g. within 24 hours) of discovering a significant security risk.

Considerations Close coordination occurs between OT, HR, IT, and physical security personnel to ensure the timely removal of high-risk individuals.

AC-3 Access Enforcement

Implementation Level **1**

Control Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

Considerations The organization ensures that access enforcement mechanisms do not adversely impact the operational performance of the OT. Example compensating controls include encapsulation (e.g. restricting the direct access to some components of an object so users cannot access state values for all of the variables of a particular object). The policy for logical access control to non-addressable and non-routable system resources and the associated information is made explicit. Access control mechanisms include hardware, firmware, and software that control the device or have device access, such as device drivers and communications controllers. Physical access control may serve as a compensating control for logical access control. However, it may not provide sufficient granularity when users require access to different functions.

AC-3(11) Access Enforcement | Restrict Access to Specific Information Types

Implementation Level: 3

Control: Restrict access to data repositories containing critical information on a need to know basis.

Considerations: The organization identifies and restricts access to information that could impact the OT environment and accounts for information types that are sensitive, proprietary, contain trade secrets, or support safety functions.

The loss of availability, integrity, and confidentiality of certain types of information that reside on a high-impact OT system may result in severe or catastrophic adverse effects on operations, assets, or individuals, including severe degradation or loss of mission capability, major damage to organizational assets, or harm to individuals involving the loss of life or life-threatening injuries.

AC-4 Information Flow Enforcement

Implementation Level: 2

Control: Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on a formally documented process.

Considerations: Information flow policy may be achieved using a combination of logical and physical flow restriction techniques. The inspection of message content may enforce information flow policy. For example, industrial OT protocols may be restricted using inbound and outbound traffic rules on a network control device between OT and IT networks. For non-routable communication, such as serial connections, devices may be configured to limit commands to and from specific tags within the OT device. The information flow policy may be supported by labelling or coloring physical connectors to aid in connecting networks. Devices that do not have a business need to communicate should not be connected (i.e. air gapped).

AC-4(4) Information Flow Enforcement | Flow Control of Encrypted Information

Implementation Level: 3

Control: Prevent encrypted information from bypassing company defined process and tools by:

a. decrypting the information;

b. terminating communications sessions attempting to pass encrypted information.

Considerations: No additional OT clarification is required for this control.

AC-5 Separation of Duties

Implementation Level **2**

Control

a. Identify and document the duties of individuals requiring separation in order to reduce the likelihood of significant exploitation; and

b. Define system access authorizations to support separation of duties.

Considerations

Example compensating controls include providing increased personnel security and auditing, divide critical functions for system management, configuration management and operations. The organization carefully considers the appropriateness of a single individual performing multiple critical roles.

AC-6 Least Privilege

Implementation Level **2**

Control

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Considerations

Example compensating controls include providing increased personnel security and auditing. The organization carefully considers the appropriateness of a single individual having multiple critical privileges. System privilege models may be tailored to enforce integrity and availability (e.g., lower privileges include read access, and higher privileges include write access).

AC-6(1) Least Privilege | Authorize Access to Security Functions

Implementation Level **2**

Control

Authorize access for individuals or roles to:

a. Security functions (deployed in hardware, software, and firmware); and

b. Security-relevant information.

Considerations

When OT components (e.g., PLCs) cannot support the logging of privileged functions, other system components within the authorization boundary may be used (e.g., engineering workstations or physical access monitoring).

AC-6(2) Least Privilege | Non-privileged Access for Nonsecurity Functions

Implementation Level 2

Control Require that users of system accounts (or roles) with access to security functions or security-relevant information use non-privileged accounts or roles, when accessing non-security functions.

Considerations When OT components (e.g., PLCs) cannot support the logging of privileged functions, other system components within the authorization boundary may be used (e.g., engineering workstations or physical access monitoring).

AC-6(3) Least Privilege | Network Access to Privileged Commands

Implementation Level 3

Control Authorize network access to specific privileged commands in terminals only for maintenance or management functions and document the rationale for such access (e.g. in the security plan for the system).

Considerations When OT components (e.g., PLCs) cannot support the logging of privileged functions, other system components within the authorization boundary may be used (e.g., engineering workstations or physical access monitoring).

AC-6(5) Least Privilege | Privileged Accounts

Implementation Level 2

Control Restrict privileged accounts on the system to authorized personnel.

Considerations When OT components (e.g., PLCs) cannot support the logging of privileged functions, other system components within the authorization boundary may be used (e.g., engineering workstations or physical access monitoring).

AC-6(7) Least Privilege | Review of User Privileges

Implementation Level 2

Control a. Review as per organizational policy (e.g. at least every 3 months) the privileges assigned to roles or classes of users with privileges to validate the need for such privileges; and

b. Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.

Considerations

No additional OT clarification is required for this control.

AC-6(9) Least Privilege | Log Use of Privileged Functions

Implementation Level 2

Control

Log the execution of privileged functions.

Considerations

When OT components (e.g., PLCs) cannot support the logging of privileged functions, other system components within the authorization boundary may be used (e.g., engineering workstations or physical access monitoring).

AC-6(10) Least Privilege | Prohibit Non-privileged Users from Executing Privileged Functions

Implementation Level 2

Control

Prevent non-privileged users from executing privileged functions.

Considerations

Example compensating controls include enhanced auditing.

AC-7 Unsuccessful Logon Attempts

Implementation Level 1

Control

a. Enforce a limit of consecutive invalid logon attempts by a user (e.g. 10 attempts) during a defined period (e.g. 30 minutes); and

b. Automatically lock the account or node until released by an administrator when the maximum number of unsuccessful attempts is exceeded. The account may be unlocked by the account owner contacting the service desk or the system administrator.

c. Automatically lock accounts if they are accessed from outside the region without informing the Service Desk or the System Administrator before travelling.

Considerations

Many OT systems remain in continuous operation, and operators remain logged onto the system at all times. A "log-over" capability may be employed. Example compensating controls include logging or recording all unsuccessful logon attempts and alerting OT security personnel through alarms or other means when the number of organization-defined consecutive invalid access attempts is exceeded. Unsuccessful logon attempt limits are enforced for accounts (e.g., administrator) or systems (e.g., engineering workstations) that are not required for continuous operation.

AC-8 System Use Notification

Implementation Level 1

Control

a. Display a logon banner/herald (if technically feasible) to users before granting access to the system that provides security notices consistent with any legal, regulatory, customer or company requirements and also include statements that:

1. Usage is governed by the IT Acceptable Use Policy and any associated guidance;
2. System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the system is prohibited; and
4. Use of the system indicates consent to monitoring and recording;

b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and

c. For publicly accessible systems:

1. Display system use information before granting further access to the publicly accessible system;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
3. Include a description of the authorized uses of the system.

Considerations

Many OT systems must remain in continuous operation, and system use notification may not be supported or effective. Example compensating controls include posting physical notices in OT facilities or providing recurring training on system use prior to permitting access.

AC-10 Concurrent Session Control

Implementation Level 3

Control

Limit the number of concurrent sessions as per organizational policy for non-privileged users (e.g. up to 5) and to system and privileged accounts(e.g. up to 2).

Considerations

No additional OT clarification is required for this control.

AC-11 Device Lock

Implementation Level: 1

Control

a. Prevent further access to the system by initiating a device lock after a defined period (e.g. 20 minutes) of inactivity and require the user to initiate a device lock before leaving the system unattended. In situations where OT cannot support authentication, or it is not advisable due to adverse impacts on safety, performance, or reliability, select compensating countermeasures; and

b. Retain the device lock until the user re-establishes access using established identification and authentication procedures.

Considerations

This control assumes a staffed environment where users interact with system displays. This control may be tailored appropriately where systems do not have displays configured, systems are placed in an access-controlled facility or locked enclosure, or immediate operator response is required in emergency situations. Example compensating controls include locating the display in an area with physical access controls that limit access to individuals with permission and need-to-know for the displayed information.

AC-11(1) Device Lock | Pattern-hiding Displays

Implementation Level: 2

Control

Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

Considerations

Physical protection may be employed to prevent access to a display or the attachment of a display. When the OT cannot conceal displayed information, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-12 Session Termination

Implementation Level: 2

Control

Automatically terminate a user session as defined in organizational policy (e.g. after 1 hour of inactivity). In situations where OT cannot support this functionality, or it is not advisable due to adverse impacts on safety, performance, or reliability, select compensating controls.

Considerations

Example compensating controls include providing increased auditing measures or limiting remote access privileges to key personnel.

AC-14 Permitted Actions Without Identification or Authentication

Implementation Level 1

Control

a. Identify user actions that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and

b. Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.

Considerations

No additional OT clarification is required for this control.

AC-16 Security and Privacy Attributes

Implementation Level 3

Control

a. Provide the means to associate critical and sensitive data with metadata tags, attributes or properties for information in storage, in process, and/or in transmission;

b. Ensure that the attribute associations are made and retained with the information;

c. Establish the following permitted security and privacy attributes for critical and sensitive data: as per company policy (e.g. Public, Confidential and Highly Confidential);

d. Determine the following permitted attribute values or ranges for each of the established attributes: as per company policy (e.g. Public, Confidential and Highly Confidential);

e. Audit changes to attributes; and

f. Review as per company policy attributes for applicability periodically (e.g. annually).

Considerations

No additional OT clarification is required for this control.

AC-17 Remote Access

Implementation Level 1

Control

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type (internal and external) of remote access allowed; and

b. Authorize each type (internal and external) of remote access to the system prior to allowing such connections.

Considerations

When the OT cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-17(1) Remote Access | Monitoring and Control

Implementation Level: 2

Control: Employ automated mechanisms to monitor and control remote access methods.

Considerations: Example compensating controls include employing nonautomated mechanisms or procedures as compensating controls. Compensating controls could include limiting remote access to a specified period of time or placing a call from the OT site to the authenticated remote entity.

AC-17(2) Remote Access | Protection of Confidentiality and Integrity Using Encryption

Implementation Level: 2

Control: Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Considerations: Encryption-based technologies should be used to support the confidentiality and integrity of remote access sessions. While OT devices often lack the ability to support modern encryption, additional devices (e.g., VPNs) can be added to support these features. This control should not be confused with SC-8 – Transmission Confidentiality and Integrity, which discusses confidentiality and integrity requirements for general communications, including between OT devices.

AC-17(3) Remote Access | Managed Access Control Points

Implementation Level: 2

Control: Route remote accesses through authorized and managed network access control points.

Considerations: Example compensating controls include connection- specific manual authentication of the remote entity.

AC-17(4) Remote Access | Privileged Commands and Access

Implementation Level: 2

Control: a. Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: System administration; and

b. Document the rationale for remote access in the security plan for the system.

Considerations No additional OT clarification is required for this control.

AC-17(9) Remote Access | Disconnect or Disable Access

Implementation Level 3

Control Provide the capability to disconnect or disable remote access to the system as defined in organizational policy (e.g. within 1 hour).

Considerations Implementation of the remote access disconnect should not impact OT operations. OT personnel should be trained on how to use the remote access disconnect.

As more OT systems become accessible remotely, the capability to disconnect or disable remote access is critical to managing risk and may be required to provide stable and safe operations.

AC-17(10) Remote Access | Authenticate Remote Commands

Implementation Level 3

Control Implement authentication and authorization mechanisms (e.g. certificates) to authenticate remote commands (e.g. certain start/stop type commands).

Considerations The ability to authenticate remote commands is important to prevent unauthorized commands that may have immediate or serious consequences, such as injury, death, property damage, the loss of high-value assets, the failure of mission or business functions, or compromise of sensitive information.

AC-18 Wireless Access

Implementation Level 1

Control a. Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and

b. Authorize each type of wireless access to the system prior to allowing such connections.

Considerations When OT cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-18(1) Wireless Access | Authentication and Encryption

Implementation Level 2

Control Protect wireless access to the system using authentication of users and/or devices.

Considerations The implementation of authentication and encryption is driven by the OT environment. If devices and users cannot all be authenticated and encrypted due to operational or technology constraints, compensating controls include providing increased auditing for wireless access, limiting wireless access privileges to key personnel, or using AC-18 (5) to reduce the boundary of wireless access.

AC-18(3) Wireless Access | Disable Wireless Networking

Implementation Level 2

Control Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.

Considerations No additional OT clarification is required for this control.

AC-18(4) Wireless Access | Restrict Configurations by Users

Implementation Level 3

Control Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.

Considerations No additional OT clarification is required for this control.

AC-18(5) Wireless Access | Antennas and Transmission Power Levels

Implementation Level 3

Control Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.

Considerations Availability and interference for wireless signals may be a concern within OT environments. Antennas and power levels should be designed to overcome and achieve availability goals. Where confidentiality is concerned, antennas and power levels can also be designed to minimize signal exposure outside of the facility.

AC-19 Access Control for Mobile Devices

Implementation Level 1

Control a. Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and

b. Authorize the connection of organizational mobile devices to organizational systems.

Considerations No additional OT clarification is required for this control.

AC-19(5) Access Control for Mobile Devices | Full Device or Container-based Encryption

Implementation Level 2

Control Employ full-device encryption or container-based encryption to protect the confidentiality and integrity of information on mobile devices.

Considerations No additional OT clarification is required for this control.

AC-20 Use of External Systems

Implementation Level 1

Control a. Establish defined terms and conditions, consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:

1. Access the system from external systems; and
2. Process, store, or transmit organization-controlled information using external systems; or

b. Prohibit the use of unapproved external systems.

Considerations Organizations refine the definition of “external” to reflect lines of authority and responsibility, the granularity of an organization entity, and their relationships. An organization may consider a system to be external if that system performs different functions, implements different policies, falls under different management authorities, or does not provide sufficient visibility into the implementation of controls to allow the establishment of a satisfactory trust relationship. For example, an OT system and a business data processing system may be considered external to each other depending on the organization's system boundaries.

Access to an OT for support by a business partner, such as a vendor or support contractor, is another common example. The definition and trustworthiness of external systems is reexamined with respect to OT functions, purposes, technology, and limitations to establish a clearly documented technical or business case for use and an acceptance of the risk inherent in the use of an external system.

AC-20(1) Use of External Systems | Limits on Authorized Use

Implementation Level 2

Control: Permit authorized individuals to use an external system to access the system or to process, store, or transmit information only after:

a. Verification of the implementation of controls on the external system as specified in the organization's security policies and security plans; or

b. Retention of approved system connection or processing agreements with the organizational entity hosting the external system.

Considerations: No additional OT clarification is required for this control.

AC-20(2) Use of External Systems | Portable Storage Devices — Restricted Use

Implementation Level 2

Control: Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.

Considerations: No additional OT clarification is required for this control.

AC-21 Information Sharing

Implementation Level 2

Control: a. Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for information sharing circumstances where user discretion is required; and

b. Employ automated mechanisms or manual processes to assist users in making information sharing and collaboration decisions.

Considerations: No additional OT clarification is required for this control.

AC-22 Publicly Accessible Content

Implementation Level 1

Control

a. Designate individuals authorized to make information publicly accessible;

b. Train authorized individuals to ensure that publicly accessible information does not contain non-public information;

c. Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and

d. Review the content on the publicly accessible system for non-public information annually and remove such information, if discovered.

Considerations

Generally, public access to OT systems is not permitted. Select information may be transferred to a publicly accessible system, possibly with added controls. The organization should review what information is being made accessible prior to publication.

AC-23 Data Mining Protection

Implementation Level 2

Control

Employ anomaly detection, access control, activity logging and encryption for databases, file servers or other critical storage systems to detect and protect against unauthorized data mining.

Considerations

No additional OT clarification is required for this control.

3 CONTROL FAMILY: AWARENESS AND TRAINING

3.1 Control Implementation Levels

Control ID	**Control** | Control Enhancement	Implementation Level		
AT-1	**Policy and Procedures**	1		
AT-2	**Literacy Training and Awareness**	1		
AT-2(2)	Insider Threat	1		
AT-2(3)	Social Engineering and Mining		2	
AT-2(4)	Suspicious Communications and Anomalous System Behavior			3
AT-3	**Role-based Training**	1		
AT-4	**Training Records**	1		

3.2 Controls

AT-1 Policy and Procedures

Implementation Level 1

Control

a. Develop, document, and disseminate to ALL users:

1. A security awareness and training policy that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Is consistent with applicable laws, customer requirements, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;

b. Designate an individual to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and

c. Review and update the current awareness and training:

1. As defined in organizational policy (e.g. every 2 years and following significant change); and

2. Procedures as per the organizational policy (e.g. annually and following significant change).

Considerations

The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

AT-2 Literacy Training and Awareness

Implementation Level: 1

Control

a. Provide security literacy training to system users (including managers, senior executives, and contractors):

1. As part of initial training for new users and regularly (e.g. annually) thereafter; and
2. When required by system changes or following the identification of new training requirements;

b. Increase the security awareness of system users (e.g. by employing the following techniques: publish articles on the Company App and Intranet; electronic training modules; posters; emails and other communications techniques);

c. Update literacy training and awareness content regulalry (e.g. annually) and following the identification of new training requirements; and

d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

Considerations

Security awareness training includes initial and periodic review of OT-specific policies, standard operating procedures, security trends, and vulnerabilities. The OT security awareness program is consistent with the requirements of the security awareness and training policy established by the organization.

AT-2(2) Literacy Training and Awareness | Insider Threat

Implementation Level: 1

Control

Provide literacy training on recognizing and reporting potential indicators of insider threat.

Considerations

No additional OT clarification is required for this control.

AT-2(3) Literacy Training and Awareness | Social Engineering and Mining

Implementation Level: 2

Control

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

Considerations

No additional OT clarification is required for this control.

AT-2(4) Literacy Training and Awareness | Suspicious Communications and Anomalous System Behavior

Implementation Level 3

Control

Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using anomalous system behavior (e.g. indicators of malicious code).

Considerations

Identify and communicate suspicious and anomalous behaviors within the OT environment. Some examples of OT suspicious or anomalous behavior may include a PLC still in programming mode when it is expected to be in run mode, process trips with an undetermined root cause, malware on an Human Machine Interface, unexpected mouse movement, or process changes that are not being performed by the operator.

Training OT personnel on potentially suspicious communications and anomalous behaviors as well as the actions to take if anomalous system behavior occurs can supplement system detection and protection mechanisms for improved response.

AT-3 Role-based Training

Implementation Level 1

Control

a. Provide role-based security training to personnel with the following roles and responsibilities: Those requiring specific Security awareness and training in order to perform their role.

1. Before authorizing access to the system, information, or performing assigned duties, and regularly (e.g. annually) thereafter; and
2. When required by system changes;

b. Update role-based training content regularly (e.g. annually) and following significant system changes or the identification of new training requirements; and

c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

Considerations

Security training includes initial and periodic review of OT-specific policies, standard operating procedures, security trends, and vulnerabilities. The OT security training program is consistent with the requirements of the security awareness and training policy established by the organization. The training may be customized for specific OT roles, which could include operators, maintainers, engineers, supervisors, and administrators.

AT-4 Training Records

Implementation Level: I

Control	a. Document and monitor information security training activities, including security awareness training and specific role-based security training; and b. Retain individual training records as defined in organizational policy (e.g. for at least 3 years).
Considerations	No additional OT clarification is required for this control.

4 CONTROL FAMILY: AUDIT AND ACCOUNTABILITY

4.1 Control Implementation Levels

Control ID	**Control** | Control Enhancement	Implementation Level		
AU-1	**Policy and Procedures**	1		
AU-2	**Event Logging**	1		
AU-3	**Content of Audit Records**	1		
AU-3(1)	Additional Audit Information		2	
AU-3(3)	Limit Personally Identifiable Information Elements		2	
AU-4	**Audit Log Storage Capacity**	1		
AU-4(1)	Transfer to Alternate Storage		2	
AU-5	**Response to Audit Logging Process Failures**	1		
AU-5(1)	Storage Capacity Warning			3
AU-5(2)	Real-time Alerts			3
AU-5(3)	Configurable Traffic Volume Thresholds		2	
AU-5(4)	Shutdown on Failure		2	
AU-5(5)	Alternate Audit Logging Capability			3
AU-6	**Audit Record Review, Analysis, and Reporting**	1		
AU-6(1)	Automated Process Integration		2	
AU-6(3)	Correlate Audit Record Repositories			3
AU-6(4)	Central Review and Analysis		2	
AU-6(5)	Integrated Analysis of Audit Records			3
AU-6(6)	Correlation with Physical Monitoring			3
AU-6(7)	Permitted Actions			3
AU-6(8)	Full Text Analysis of Privileged Commands			3
AU-6(9)	Correlation with Information from Nontechnical Sources			3
AU-7	**Audit Record Reduction and Report Generation**			3
AU-7(1)	Automatic Processing		2	
AU-8	**Time Stamps**	1		
AU-9	**Protection of Audit Information**	1		
AU-9(2)	Store on Separate Physical Systems or Components			3
AU-9(3)	Cryptographic Protection			3
AU-9(4)	Access by Subset of Privileged Users		2	
AU-10	**Non-repudiation**			3
AU-11	**Audit Record Retention**	1		
AU-12	**Audit Record Generation**	1		
AU-12(1)	System-wide and Time-correlated Audit Trail			3

Control ID	Control | Control Enhancement	Implementation Level		
AU-12(3)	Changes by Authorized Individuals			3

4.2 Controls

AU-1 Policy and Procedures

Implementation Level: 1

Control

a. Develop, document, and disseminate to appropriate personnel or roles:

1. An Organization-level, Business process-level or System-level audit and accountability policy that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Is consistent with applicable laws, customer requirements, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;

b. Designate an individual to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and

c. Review and update the current audit and accountability:

1. As defined in organizational policy (e.g. at least every 2 years and following significant change); and

2. Procedures as per organizational policy (e.g. annually and following significant change).

Considerations

The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

AU-2 Event Logging

Implementation Level: 1

Control

a. Identify the types of events that the system is capable of logging in support of the audit function: Examples include: firmware updates, configuration changes in production requirement (e.g. safety sensitive machine settings, enabling wireless connectivity, "auto start" functionality), account creation/modification, logon/logoff activity; failed access attempts and security policy changes.

b. Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

c. Specify the following event types for logging within the system: events that are significant and relevant to the security of the system.

d. Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and

e. Review and update the event types selected for logging regularly (e.g. annually) or where appropriate following an incident.

Considerations Organizations may want to include relevant OT events (e.g., alerts, alarms, configuration and status changes, operator actions) in their event logging, which may be designated as audit events.

AU-3 Content of Audit Records

Implementation Level 1

Control Ensure that audit records contain information that establishes the following:

a. What type of event occurred;

b. When the event occurred;

c. Where the event occurred;

d. Source of the event;

e. Outcome of the event; and

f. Identity any individuals, subjects, or objects/entities associated with the event.

Considerations No additional OT clarification is required for this control.

AU-3(1) Content of Audit Records | Additional Audit Information

Implementation Level 2

Control Generate audit records containing the following additional information: Any additional audit information that may be required in addition to the baseline stated by the Security Operations Centre or required by the Authority/Regulator.

Considerations No additional OT clarification is required for this control.

AU-3(3) Content of Audit Records | Limit Personally Identifiable Information Elements

Implementation Level 2

Control Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: Email or Name.

Considerations No additional OT clarification is required for this control.

AU-4 Audit Log Storage Capacity

Implementation Level 1

Control Allocate audit log storage capacity to accommodate logging to satisfy the audit log retention requirements.

Considerations No additional OT clarification is required for this control.

AU-4(1) Audit Log Storage Capacity | Transfer to Alternate Storage

Implementation Level 2

Control Transfer audit logs:

a. If networked connected, as per organizational policy (e.g. at least quarterly); or

b. If standalone then by default no log transfers are necessary; unless a risk assessment, business requirement or capacity limitation requires this to be undertaken more frequently (e.g. during the next planned maintenance).

Considerations No additional OT clarification is required for this control.

Organizational requirements may require the storage of very large amounts of data, which OT components may not be able to support directly.

AU-5 Response to Audit Logging Process Failures

Implementation Level 1

Control a. Alert the local Security Operations Centre (where the system is monitored by the SOC), information system owner and/or system administrator within defined organizational policies (e.g. as soon as detected) if log collection is automated, otherwise during the next planned maintenance in the event of an audit logging process failure; and

b. Take the following additional actions: Information system continues operation and information system owner and/or system administrator takes corrective action to address the cause of failure; an incident shall be raised in ITSM or Risk Management system.

Considerations No additional OT clarification is required for this control.

AU-5(1) Response to Audit Logging Process Failures | Storage Capacity Warning

Implementation Level **3**

Control: Provide a warning to the system owner or system administrator as soon as allocated audit log storage volume reaches defined repository maximum threshhold (e.g. 80% of audit log storage capacity) and raise an incident in ITSM system.

Considerations: No additional OT clarification is required for this control.

AU-5(2) Response to Audit Logging Process Failures | Real-time Alerts

Implementation Level **3**

Control: Provide an alert as per organizational policy (e.g. after 3 unsuccessfull attempts) to Security Operations Centre (where the system is monitored by the SOC), information system owner and/or system administrator when the following audit failure events occur: log data is not delivered or log data is incomplete.

Considerations: No additional OT clarification is required for this control.

AU-5(3) Response to Audit Logging Process Failures | Configurable Traffic Volume Thresholds

Implementation Level **2**

Control: Enforce configurable network communications traffic volume thresholds reflecting limits on audit log storage capacity and delay network traffic above those thresholds.

Considerations: No additional OT clarification is required for this control.

AU-5(4) Response to Audit Logging Process Failures | Shutdown on Failure

Implementation Level **2**

Control: Invoke a degraded operational mode with limited mission or business functionality available in the event of system audit logging failures, unless an alternate audit logging capability exists.

Considerations: No additional OT clarification is required for this control.

AU-5(5) Response to Audit Logging Process Failures | Alternate Audit Logging Capability

Implementation Level 3

Control: Provide an alternate audit logging capability in the event of a failure in primary audit logging capability that implements similar logging capabilities and meets the service levels.

Considerations: No additional OT clarification is required for this control.

AU-6 Audit Record Review, Analysis, and Reporting

Implementation Level 1

Control: a. Review and analyse system audit records as per organizational policy (e.g at least quarterly); unless a risk assessment, business requirement or capacity limitation requires this to be more frequent for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity;

Audit records or related events from OT Systems which are not automatically forwarded to a SOC, or Security Information and Event Management (SIEM) tool shall be reviewed by an appropriate independent person/team as a minimum:

1. Networked devices – e.g. quarterly
2. Standalone devices – e.g. by default no logs are required; or unless a risk assessment, business requirement or capacity limitation requires this to be undertaken e.g. during the next planned maintenance.

b. Report findings to the local Security Operations Centre (where the system is monitored by the SOC); information system owner; and/or system administrator; and

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.

Considerations: No additional OT clarification is required for this control.

AU-6(1) Audit Record Review, Analysis, and Reporting | Automated Process Integration

Implementation Level 2

Control: Integrate audit record review, analysis, and reporting processes using automated systems utilized by the Security Operations Centre or Business managed capability run locally.

Considerations Example compensating controls include manual mechanisms or procedures. For devices where audit records cannot be feasibly collected, periodic manual review may be necessary.

AU-6(3) Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories

Implementation Level 3

Control Analyse and correlate audit records across different repositories to gain organization-wide situational awareness.

Considerations No additional OT clarification is required for this control.

AU-6(4) Audit Record Review, Analysis, and Reporting | Central Review and Analysis

Implementation Level 2

Control Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.

Considerations No additional OT clarification is required for this control.

AU-6(5) Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records

Implementation Level 3

Control Integrate analysis of audit records with analysis of vulnerability scanning information, system monitoring information, system health information and threat intelligence data to further enhance the ability to identify inappropriate or unusual activity.

Considerations No additional OT clarification is required for this control.

AU-6(6) Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring

Implementation Level 3

Control Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

Considerations No additional OT clarification is required for this control.

AU-6(7) Audit Record Review, Analysis, and Reporting | Permitted Actions

Implementation Level 3

Control Specify the permitted actions for each system process, system roles and users associated with the review, analysis, and reporting of audit record information.

Considerations No additional OT clarification is required for this control.

AU-6(8) Audit Record Review, Analysis, and Reporting | Full Text Analysis of Privileged Commands

Implementation Level 3

Control Perform a full text analysis of logged privileged commands in a physically distinct component or subsystem of the system, or other system that is dedicated to that analysis.

Considerations No additional OT clarification is required for this control.

AU-6(9) Audit Record Review, Analysis, and Reporting | Correlation with Information from Nontechnical Sources

Implementation Level 3

Control Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.

Considerations No additional OT clarification is required for this control.

AU-7 Audit Record Reduction and Report Generation

Implementation Level 3

Control Provide and implement an audit record reduction and report generation capability that:

a. Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and

b. Does not alter the original content or time ordering of audit records.

Considerations No additional OT clarification is required for this control.

AU-7(1) Audit Record Reduction and Report Generation | Automatic Processing

Implementation Level **2**

Control Provide and implement the capability to process, sort, and search audit records for events of interest.

Considerations No additional OT clarification is required for this control.

AU-8 Time Stamps

Implementation Level **1**

Control a. Use internal system clocks to generate time stamps for audit records; and

b. Record time stamps for audit records that meet Security Operations Centre or Technical Authority defined granularity requirements and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

Considerations Example compensating controls include using a separate system designated as an authoritative time source. See related control SC-45.

AU-9 Protection of Audit Information

Implementation Level **1**

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

b. Alert the Security Operations Centre (where the system is monitored by the SOC), information system owner and/or system administrator; raise an incident in ITSM or Risk Management system upon detection of unauthorized access, modification, or deletion of audit information.

Considerations No additional OT clarification is required for this control.

AU-9(2) Protection of Audit Information | Store on Separate Physical Systems or Components

Implementation Level 3

Control Store audit records as per organizational policy (e.g. for at least 12 months) or as required by regulator in a repository that is part of a physically different system or system component than the system or component being audited.

Considerations No additional OT clarification is required for this control.

AU-9(3) Protection of Audit Information | Cryptographic Protection

Implementation Level 3

Control Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.

Considerations No additional OT clarification is required for this control.

AU-9(4) Protection of Audit Information | Access by Subset of Privileged Users

Implementation Level 2

Control Authorize access to management of audit logging functionality to only permitted system administrators or other permitted users (e.g. those responsible for reviewing audit logs).

Considerations No additional OT clarification is required for this control.

AU-10 Non-repudiation

Implementation Level 3

Control Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed the actions or activities that resulted in an impact of Confidentiality, Integrity or Availabilty.

Considerations No additional OT clarification is required for this control.

AU-11 Audit Record Retention

Implementation Level 1

Control Retain audit records for a period agreed with the information system owner and/or system regulator to provide support for after-the-fact investigations of incidents and to meet legal, regulatory, customer and organizational information retention requirements.

Considerations No additional OT clarification is required for this control.

AU-12 Audit Record Generation

Implementation Level 1

Control a. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on Assets that are capable of generating such information;

b. Allow permitted personnel or roles to select the event types that are to be logged by specific components of the system; and

c. Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

Considerations No additional OT clarification is required for this control.

AU-12(1) Audit Record Generation | System-wide and Time-correlated Audit Trail

Implementation Level 3

Control Compile audit records from different systems and users into a system-wide (logical or physical) audit trail that is time-correlated to within default time zone for the relationship between time stamps of individual records in the audit trail.

Considerations Example compensating controls include providing time-correlated audit records on a separate system.

AU-12(3) Audit Record Generation | Changes by Authorized Individuals

Implementation Level 3

Control Provide and implement the capability for sytem administrator to change the logging to be performed on all systems and components based on system and security events in

	near real-time.
Considerations	Example compensating controls include employing nonautomated mechanisms or procedures.

5 CONTROL FAMILY: SECURITY ASSESSMENT AND AUTHORISATION

5.1 Control Implementation Levels

Control ID	Control | Control Enhancement	Implementation Level		
CA-1	**Policy and Procedures**	1		
CA-2	**Control Assessments**	1		
CA-2(1)	Independent Assessors		2	
CA-2(2)	Specialized Assessments			3
CA-3	**Information Exchange**	1		
CA-3(6)	**Information Exchange | Transfer Authorizations**			3
CA-5	**Plan of Action and Milestones**	1		
CA-6	**Authorization**	1		
CA-7	**Continuous Monitoring**	1		
CA-7(1)	Independent Assessment		2	
CA-7(4)	Risk Monitoring		2	
CA-8	**Penetration Testing**			3
CA-8(1)	Independent Penetration Testing Agent or Team			3
CA-8(2)	Red Team Exercises			3
CA-9	**Internal System Connections**	1		

5.2 Controls

CA-1 Policy and Procedures

Implementation Level 1

Control a. Develop, document, and disseminate to appropriate personnel or roles:

1. Organization-level; Business process-level; System-level assessment, authorization, and monitoring policy that:

    a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

    b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the assessment, authorization,

and monitoring policy and the associated assessment, authorization, and monitoring controls;

b. Designate an individual to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and

c. Review and update the current assessment, authorization, and monitoring:

1. As defined in organizational policy (e.g. every 2 years and following significant change); and

2. Procedures as per organizational policy (e.g. annually and following significant change).

Considerations The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

CA-2 Control Assessments

Implementation Level | I

Control a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;

b. Develop a control assessment plan that describes the scope of the assessment including:

1. Controls and control enhancements under assessment;

2. Assessment procedures to be used to determine control effectiveness; and

3. Assessment environment, assessment team, and assessment roles and responsibilities;

c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;

d. Assess the controls in the system and its environment of operation regularly (e.g. at least annually), or as required by Security Team to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements;

e. Produce a control assessment report that document the results of the assessment; and

f. Provide the results of the control assessment to: Authorizing Official; Security Team; Information System Owner; Internal Audit; Security Authority.

Considerations Assessments are performed and documented by qualified assessors (i.e. experienced in assessing OT) authorized by the organization. The individual or group conducting the assessment fully understands the organizational information security policies and procedures, the OT security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. The organization ensures that the assessment does not affect system operation or result in unintentional system modification. If assessment activities must be performed on the production OT, it may need to be taken offline before an assessment can be conducted, or the assessment should be scheduled to occur during planned OT outages whenever possible.

CA-2(1) Control Assessments | Independent Assessors

Implementation Level 2

Control: Employ independent assessors or assessment teams to conduct control assessments.

Considerations: No additional OT clarification is required for this control.

CA-2(2) Control Assessments | Specialized Assessments

Implementation Level 3

Control: Include as part of control assessments as per organizational policy (e.g. at least annually) announced:

a. security instrumentation;

b. malicious user testing;

c. insider threat assessment;

d. data leakage or data loss assessment;

e. pen-testing;

f. SOC assessment;

or table top exercises covering those topics.

Considerations: The organization conducts risk analysis to support the selection of an assessment target (e.g., the live system, an offline replica, or lab system).

CA-3 Information Exchange

Implementation Level 1

Control: a. Approve and manage the exchange of information between the system and other systems using appropriate documentation, for example: memoranda of understanding or agreement; service level agreements (SLAs); nondisclosure agreements (NDAs), code of connection.

b. Document, as part of each exchange agreement, the interface characteristics, security requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and

c. Review and update the agreements regularly (e.g. at least annually) or following significant change.

Considerations: Organizations perform risk-benefit analysis to determine whether an OT should be connected to other systems. The authorizing official (AO) fully understands the organizational information security policies and procedures; the OT security policies and procedures; the risks to organizational operations and assets, individuals, other organizations, and the Nation associated with the connection to other systems; the individuals and organizations that operate and maintain the systems, including maintenance contractors or service providers; and the specific health, safety, and environmental risks associated with a particular interconnection.

Connections from the OT environment to other security zones may cross the authorization boundary such that two different authorizing officials may be required to approve the connection. Decisions to accept risk are documented.

CA-3(6) Information Exchange | Transfer Authorizations

Implementation Level 3

Control: Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e. write permissions or privileges) prior to accepting such data.

Considerations: No additional OT clarification is required for this control.

CA-5 Plan of Action and Milestones

Implementation Level 1

Control: a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and

b. Update existing plan of action and milestones as per organizational policy (e.g. monthly) based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Considerations: Corrective actions identified in assessments may not be immediately actionable in an OT environment. Therefore, short-term mitigations may be implemented to reduce risk as part of the gap closure plan or plan of action and milestones.

CA-6 Authorization

Implementation Level 1

Control: a. Assign a senior official as the authorizing official for the system;

b. Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;

c. Ensure that the authorizing official for the system, before commencing operations:

1. Accepts the use of common controls inherited by the system; and
2. Authorizes the system to operate;

d. Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;

e. Update the authorizations regularly (e.g. at least on an annual basis).

Considerations No additional OT clarification is required for this control.

CA-7 Continuous Monitoring Implementation Level 1

Control a. Establishing the following system-level metrics to be monitored: Metrics agreed with the Security Operations Centre or local Business equivalent where applicable and agreed with Architecture Design Authority.

b. Establishing frequencies for monitoring and frequencies for assessment of control effectiveness;

c. Ongoing control assessments in accordance with the continuous monitoring strategy;

d. Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;

e. Correlation and analysis of information generated by control assessments and monitoring;

f. Response actions to address results of the analysis of control assessment and monitoring information; and

g. Reporting the security status of the system to the Security Operations Centre or local Business equivalent in line with the established requirements.

Considerations Continuous monitoring programs for OT are designed, documented, and implemented with input from OT personnel. The organization ensures that continuous monitoring does not interfere with OT functions. The individual or group designing and conducting the continuous monitoring for the OT systems implements a monitoring program that is consistent with the organizational information security policies and procedures, the OT security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. Continuous monitoring can be automated or manual at a frequency sufficient to support risk-based decisions. For example, the organization may monitor event logs manually on a specified frequency less often for lower-risk, isolated systems than for higher-risk, networked systems.

CA-7(1) Continuous Monitoring | Independent Assessment Implementation Level 2

Control Employ independent assessors or assessment teams to monitor the controls in the system regulalry (e.g. on an annual basis).

Considerations No additional OT clarification is required for this control.

CA-7(4) Continuous Monitoring | Risk Monitoring

Implementation Level 2

Control Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following:

a. Effectiveness monitoring;

b. Compliance monitoring; and

c. Change monitoring.

Considerations No additional OT clarification is required for this control.

CA-8 Penetration Testing

Implementation Level 3

Control Conduct penetration testing regulalry (e.g. at least annually) on all critical systems, components and applications.

Considerations No additional OT clarification is required for this control.

CA-8(1) Penetration Testing | Independent Penetration Testing Agent or Team

Implementation Level 3

Control Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.

Considerations No additional OT clarification is required for this control.

CA-8(2) Penetration Testing | Red Team Exercises

Implementation Level 3

Control

Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement:

a. social engineering attack

b. malware deployment

c. exfiltrate data

Considerations

No additional OT clarification is required for this control.

CA-9 Internal System Connections

Implementation Level 1

Control

a. Authorize internal connections of system components or classes of components to the system;

b. Document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated;

c. Terminate internal system connections after the connected components cease being part of the organizational system; and

d. Review the continued need for each internal connection regularly (e.g. annually).

Considerations

Organizations perform risk-benefit analysis to determine whether OT equipment should be connected to other internal system components and then document those connections. The AO fully understands the potential risks associated with approving individual connections or approving a class of components to be connected. For example, the AO may broadly approve the connection of any sensors limited to 4 to 20 milliamp (mA) communication, while other connection types (e.g., serial or Ethernet) require individual approval. Decisions to accept risk are documented.

6 CONTROL FAMILY: CONFIGURATION MANAGEMENT

6.1 Control Implementation Levels

Control ID	Control | Control Enhancement	Implementation Level		
CM-1	**Policy and Procedures**	1		
CM-2	**Baseline Configuration**	1		
CM-2(2)	Automation Support for Accuracy and Currency		2	
CM-2(3)	Retention of Previous Configurations		2	
CM-2(7)	Configure Systems and Components for High-risk Areas		2	
CM-3	**Configuration Change Control**		2	
CM-3(1)	Automated Documentation, Notification, and Prohibition of Changes			3
CM-3(2)	Testing, Validation, and Documentation of Changes		2	
CM-3(4)	Security and Privacy Representatives		2	
CM-3(6)	Cryptography Management			3
CM-4	**Impact Analyses**	1		
CM-4(1)	Separate Test Environments			3
CM-4(2)	Verification of Controls		2	
CM-5	**Access Restrictions for Change**	1		
CM-5(1)	Automated Access Enforcement and Audit Records			3
CM-6	**Configuration Settings**	1		
CM-6(1)	Automated Management, Application, and Verification			3
CM-6(2)	Respond to Unauthorized Changes			3
CM-7	**Least Functionality**	1		
CM-7(1)	Periodic Review		2	
CM-7(2)	Prevent Program Execution		2	
CM-7(4)	Unauthorized Software — Deny-by-exception			3
CM-7(5)	Authorized Software — Allow-by-exception		2	
CM-8	**System Component Inventory**	1		
CM-8(1)	Updates During Installation and Removal		2	
CM-8(2)	Automated Maintenance			3
CM-8(3)	Automated Unauthorized Component Detection		2	
CM-8(4)	Accountability Information			3
CM-9	**Configuration Management Plan**		2	
CM-10	**Software Usage Restrictions**	1		
CM-11	**User-installed Software**	1		

CM-12	**Information Location**		2	
CM-12(1)	Automated Tools to Support Information Location		2	

6.2 Controls

CM-1 Policy and Procedures

Implementation Level 1

Control

a. Develop, document, and disseminate to appropriate personnel or roles:

1. An Organization, Mission/business process, System level (as appropriate) configuration management policy that:

(a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(b) Is consistent with applicable laws, directives, regulations, customer requirements, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;

b. Designate an individual to manage the development, documentation, and dissemination of the configuration management policy and procedures; and

c. Review and update the current configuration management:

1. As defined in organizational policy (e.g. every 2 years) and following significant change; and

2. Procedures as per organizational policy (e.g. annually) and following significant change.

Considerations

The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

CM-2 Baseline Configuration

Implementation Level 1

Control

a. Develop, document, and maintain under configuration control, a current baseline configuration of the system; and

b. Review and update the baseline configuration of the system, e.g.:

1. At least annually;

2. When required due to significant change; and

3. When system components are installed or upgraded.

Considerations No additional OT clarification is required for this control.

CM-2(2) Baseline Configuration | Automation Support for Accuracy and Currency

Implementation Level 2

Control Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using automated mechanisms.

Considerations No additional OT clarification is required for this control.

CM-2(3) Baseline Configuration | Retention of Previous Configurations

Implementation Level 2

Control Retain previous versions of baseline configurations of the system to support rollback as per organizational policy (e.g. at least two).

Considerations No additional OT clarification is required for this control.

CM-2(7) Baseline Configuration | Configure Systems and Components for High-risk Areas

Implementation Level 2

Control a. Issue devices (e.g. laptops, mobile phones) including approved IT/OT devices (e.g. wearable technology, printers, cameras and other "smart devices") with default configuration containing no company-specific configuration or data to individuals traveling to locations that the organization deems to be of significant risk; and

b. Apply the following controls to the systems or components when the individuals return from travel: The assets in question should either be left with Company staff in country, or returned to IT/OT teams for secure sanitisation or destruction in accordance with the classification of data (both company and 3rd party) held on the asset and/or any contractual obligations.

Considerations No additional OT clarification is required for this control.

CM-3 Configuration Change Control

Implementation Level **2**

Control

a. Determine and document the types of changes to the system that are configuration-controlled;

b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security impact analyses;

c. Document configuration change decisions associated with the system;

d. Implement approved configuration-controlled changes to the system;

e. Retain records of configuration-controlled changes to the system as defined in organizational policy (e.g. at least 1 year) or in any contractual obligations;

f. Monitor and review activities associated with configuration-controlled changes to the system; and

g. Coordinate and provide oversight for configuration change control activities through a formal change board (e.g. Change Advisory Board) that convenes weekly; or as required to support the business' change timescales.

Considerations

No additional OT clarification is required for this control.

CM-3(1) Configuration Change Control | Automated Documentation, Notification, and Prohibition of Changes

Implementation Level **3**

Control

Use an ITSM system or other mechanism to:

a. Document proposed changes to the system;

b. Notify the change board of proposed changes to the system and request change approval;

c. Highlight proposed changes to the system that have not been approved or disapproved (e.g. within 24 hours);

d. Prohibit changes to the system until designated approvals are received;

e. Document all changes to the system; and

f. Notify the change board and system owner when approved changes to the system are completed.

Considerations

No additional OT clarification is required for this control.

CM-3(2) Configuration Change Control | Testing, Validation, and Documentation of Changes

Implementation Level **2**

Control

Test, validate, and document changes to the system before finalizing the implementation of the changes.

Considerations No additional OT clarification is required for this control.

CM-3(4) Configuration Change Control | Security and Privacy Representatives

Implementation Level 2

Control Require security representatives to be members of the change board.

Considerations No additional OT clarification is required for this control.

CM-3(6) Configuration Change Control | Cryptography Management

Implementation Level 3

Control Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: data encryption at rest and in transit, digital signatures and key management.

Considerations No additional OT clarification is required for this control.

CM-4 Impact Analyses

Implementation Level 1

Control Analyse changes to the system to determine potential security impacts prior to change implementation.

Considerations The organization considers OT safety and security interdependencies. OT security and safety personnel are included in change process management if the change to the system may impact safety or security.

CM-4(1) Impact Analyses | Separate Test Environments

Implementation Level 3

Control Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.

Considerations No additional OT clarification is required for this control.

CM-4(2) Impact Analyses | Verification of Controls

Implementation Level **2**

Control After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.

Considerations No additional OT clarification is required for this control.

CM-5 Access Restrictions for Change

Implementation Level **1**

Control Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.

Considerations Some OT devices allow for the configuration and use of mode change switches. Where available, these should be used to prevent unauthorized changes. For example, many PLCs have key switches that allow the device to be placed in a programming mode or a running mode. Those PLCs should be placed in a running or remote mode to prevent unauthorized programming changes, and the key should be removed from the key switch and managed appropriately.

CM-5(1) Access Restrictions for Change | Automated Access Enforcement and Audit Records

Implementation Level **3**

Control a. Enforce access restrictions using automated mechanisms; and

b. Automatically generate audit records of the enforcement actions.

Considerations No additional OT clarification is required for this control.

CM-6 Configuration Settings

Implementation Level: 1

Control

a. Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using common secure configurations;

b. Implement the configuration settings;

c. Identify, document, and approve any deviations from established configuration settings for system components based on operational requirements; and

d. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Considerations

No additional OT clarification is required for this control.

CM-6(1) Configuration Settings | Automated Management, Application, and Verification

Implementation Level: 3

Control

Manage, apply, and verify configuration settings for system, firmware and Operating System components using configuration management tool.

Considerations

No additional OT clarification is required for this control.

CM-6(2) Configuration Settings | Respond to Unauthorized Changes

Implementation Level: 3

Control

Take the following actions in response to unauthorized changes to system components: alert Security Operation Centre and system administrator and raise incident in ITSM system.

Considerations

No additional OT clarification is required for this control.

CM-7 Least Functionality

Implementation Level: 1

Control

a. Configure the system to provide only essential capabilities.

b. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services:

1. Insecure or unauthenticated protocols that are not approved as part of an

asset standard build.

2. Instant messaging or chat software that is not approved as part of the asset standard build.

3. Unused ports and protocols.

Considerations The organization implements least functionality by allowing only the specified functions, protocols, and/or services required for OT operations. For non-routable protocols, such as serial communications, interrupts could be disabled or set points could be made read- only except for privileged users to limit functionality. Ports are part of the address space in network protocols and are often associated with specific protocols or functions. For routable protocols, ports can be disabled on many networking devices to limit functionality to the minimum required for operation.

CM-7(1) Least Functionality | Periodic Review

Implementation Level 2

Control a. Review the system as per organizational policy (e.g. annually) or following an Incident to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and

b. Disable or remove functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

Considerations No additional OT clarification is required for this control.

CM-7(2) Least Functionality | Prevent Program Execution

Implementation Level 2

Control Prevent program execution in accordance with policies, rules of behaviour, and/or access agreements regarding software program usage and restrictions; rules authorizing the terms and conditions of software program usage.

Considerations No additional OT clarification is required for this control.

CM-7(4) Least Functionality | Unauthorized Software - Deny-by-exception

Implementation Level 3

Control a. Identify software programs not authorized to execute on the system;

b. Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and

c. Review and update the list of unauthorized software programs regulalrly (e.g. at least annually).

Considerations No additional OT clarification is required for this control.

CM-7(5) Least Functionality | Authorized Software - Allow-by-exception

Implementation Level 2

Control a. Identify software programs authorized to execute on the system;

b. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and

c. Review and update the list of authorized software programs as per organizational policy (e.g. at least every 6 months).

Considerations The set of applications that run in OT is relatively static, making allowlisting practical.

CM-8 System Component Inventory

Implementation Level 1

Control a. Develop and document an inventory of system components that:

1. Accurately reflects the system;

2. Includes all components within the system;

3. Does not include duplicate accounting of components or components assigned to any other system;

4. Is at the level of granularity deemed necessary for tracking and reporting; and

5. Includes the following information to achieve system component accountability: Configuration Item Name; Type; Location; Process; Device Group; System Name*; Network**, Device ID/Asset Tag; Device Name; Serial Number; Vendor/ Manufacturer; Model/Product Name; Firmware/Software information; Date of Receipt; Cost; Stage; Status; Description; Device Reference; Last Seen.

* *This reference shall match the name convention of the (IT/OT) System assigned by System Owner, Authorising Official (AO) etc.*

** *Additional fields for Network Connectivity arrangements (e.g. addresses, ports, connection type, network protocols (Modbus, TCP, Profinet), encryption) for network connected devices or indicate device is Standalone.*

b. Review and update the system component inventory as items change.

Considerations No additional OT clarification is required for this control.

CM-8(1) System Component Inventory | Updates During Installation and Removal

Implementation Level 2

Control: Update the inventory of system components as part of component installations, removals, and system updates.

Considerations: No additional OT clarification is required for this control.

CM-8(2) System Component Inventory | Automated Maintenance

Implementation Level 3

Control: Maintain the currency, completeness, accuracy, and availability of the inventory of system components using ITSM and asset discovery tools.

Considerations: No additional OT clarification is required for this control.

CM-8(3) System Component Inventory | Automated Unauthorized Component Detection

Implementation Level 2

Control:

a. Detect the presence of unauthorized hardware, software, and firmware components within the system using automated mechanisms as per organizational policy (e.g. on a monthly basis); and

b. Take the following actions when unauthorized components are detected: disable network access by such components; isolate the components; initiate Company incident response processes; raise an incident in ITSM system.

Considerations: No additional OT clarification is required for this control.

CM-8(4) System Component Inventory | Accountability Information

Implementation Level 3

Control: Include in the system component inventory information, a means for identifying by: name; position; or role, individuals responsible and accountable for administering those components.

Considerations: No additional OT clarification is required for this control.

CM-9 Configuration Management Plan

Implementation Level 2

Control Develop, document, and implement a configuration management plan for the system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;

c. Defines the configuration items for the system and places the configuration items under configuration management;

d. Is reviewed and approved by appropriate personnel or roles; and

e. Protects the configuration management plan from unauthorized disclosure and modification.

Considerations Configuration management plans apply to the internal and external (e.g., contractors, integrators) resources responsible for device configuration.

CM-10 Software Usage Restrictions

Implementation Level 1

Control a. Use software and associated documentation in accordance with contract agreements and copyright laws;

b. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Considerations No additional OT clarification is required for this control.

CM-11 User-installed Software

Implementation Level 1

Control a. Establish policies governing the installation of software by users;

b. Enforce software installation policies through the following methods: automated or procedural means; and

c. Monitor policy compliance as per organizational polciry (e.g. at least every 6 months), with non-compliance being raised as an Incident within ITSM or Risk Management tool.

Considerations No additional OT clarification is required for this control.

CM-12 Information Location

Implementation Level 2

Control a. Identify and document the location of information and the specific system components on which the information is processed and stored;

b. Identify and document the users who have access to the system and system components where the information is processed and stored; and

c. Document changes to the location (i.e. system or system components) where the information is processed and stored.

Considerations Organizations identify specific information types or components to track where information is being processed and stored. Information to consider in the OT environment may include shared account passwords, PLC backup files, detailed network drawings, and risk assessments that identify specific threats with the environment.

CM-12(1) Information Location | Automated Tools to Support Information Location

Implementation Level 2

Control Use automated tools to identify information by information type on system components to ensure controls are in place to protect organizational information.

Considerations No additional OT clarification is required for this control.

7 CONTROL FAMILY: CONTINGENCY PLANNING

7.1 Control Implementation Levels

Control ID	Control | Control Enhancement	Implementation Level		
CP-1	**Policy and Procedures**	1		
CP-2	**Contingency Plan**	1		
CP-2(1)	Coordinate with Related Plans		2	
CP-2(2)	Capacity Planning			3
CP-2(3)	Resume Mission and Business Functions		2	
CP-2(5)	Continue Mission and Business Functions			3
CP-2(8)	Identify Critical Assets		2	
CP-3	**Contingency Training**	1		
CP-3(1)	Simulated Events			3
CP-4	**Contingency Plan Testing**	1		
CP-4(1)	Coordinate with Related Plans		2	
CP-4(2)	Alternate Processing Site			3
CP-6	**Alternate Storage Site**		2	
CP-6(1)	Separation from Primary Site		2	
CP-6(2)	Recovery Time and Recovery Point Objectives			3
CP-6(3)	Accessibility		2	
CP-7	**Alternate Processing Site**		2	
CP-7(1)	Separation from Primary Site		2	
CP-7(2)	Accessibility		2	
CP-7(3)	Priority of Service		2	
CP-7(4)	Preparation for Use			3
CP-8	**Telecommunications Services**		2	
CP-8(1)	Priority of Service Provisions		2	
CP-8(2)	Single Points of Failure		2	
CP-8(3)	Separation of Primary and Alternate Providers			3
CP-8(4)	Provider Contingency Plan			3
CP-9	**System Backup**	1		
CP-9(1)	Testing for Reliability and Integrity		2	
CP-9(2)	Test Restoration Using Sampling			3
CP-9(3)	Separate Storage for Critical Information			3
CP-9(5)	Transfer to Alternate Storage Site			3
CP-9(8)	Cryptographic Protection		2	
CP-10	**System Recovery and Reconstitution**	1		

Control ID	Control | Control Enhancement	Implementation Level		
CP-10(2)	Transaction Recovery		2	
CP-10(4)	Restore Within Time Period			3
CP-10(6)	Component Protection		2	
CP-12	**Safe Mode**	1		

7.2 Controls

CP-1 Policy and Procedures

Implementation Level: 1

Control

a. Develop, document, and disseminate to appropriate personnel or roles:

1. An organization-level contingency planning policy that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Is consistent with applicable laws, customer requirements, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;

b. Designate an individual to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

c. Review and update the current contingency planning:

1. As defined in organizational policy (e.g. every 2 years) and following significant change; and

2. Procedures as per organizational policy (e.g. annually) and following significant change.

Considerations

The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

CP-2 Contingency Plan

Implementation Level: 1

Control

a. Develop a contingency plan for the system that:

1. Identifies essential mission and business functions and associated contingency requirements;

2. Provides recovery objectives, restoration priorities, and metrics;

3. Addresses contingency roles, responsibilities, assigned individuals with contact information;

4. Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;

5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;

6. Addresses the sharing of contingency information; and

7. Is reviewed and approved by an authorizing official or designated representative;

b. Distribute copies of the contingency plan to appropriate recipients, which shall include but not be limited to: service providers; Business Continuity staff; information systems owners.

c. Coordinate contingency planning activities with incident handling activities;

d. Review the contingency plan for the system regulalry (e.g. at least annually);

e. Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;

f. Communicate contingency plan changes to appropriate recipients, which shall include but not be limited to: service providers; Business Continuity staff; information system owners.

g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and

h. Protect the contingency plan from unauthorized disclosure and modification.

Considerations The organization defines contingency plans for categories of disruptions or failures. In the case of a contingency, the OT equipment executes preprogrammed functions, such as alerting the operator of the failure and then doing nothing, alerting the operator and then safely shutting down the industrial process, or alerting the operator and then maintaining the last operational setting prior to failure. Contingency plans for widespread disruption may involve specialized organizations (e.g., FEMA, emergency services, regulatory authorities).

CP-2(1) Contingency Plan | Coordinate with Related Plans

Implementation Level 2

Control Coordinate contingency plan development with organizational elements responsible for related plans (e.g. Business Continuity Plan, Disaster Recovery Plan, Incident Response Plan).

Considerations No additional OT clarification is required for this control.

CP-2(2) Contingency Plan | Capacity Planning

Implementation Level: 3

Control: Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

Considerations: No additional OT clarification is required for this control.

CP-2(3) Contingency Plan | Resume Mission and Business Functions

Implementation Level: 2

Control: Plan for the resumption of critical mission and business functions within a time period acceptable to the business of contingency plan activation.

Considerations: No additional OT clarification is required for this control.

CP-2(5) Contingency Plan | Continue Mission and Business Functions

Implementation Level: 3

Control: Plan for the continuance of all mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.

Considerations: No additional OT clarification is required for this control.

CP-2(8) Contingency Plan | Identify Critical Assets

Implementation Level: 2

Control: Identify critical system assets supporting critical mission and business functions.

Considerations: No additional OT clarification is required for this control.

CP-3 Contingency Training

Implementation Level: 1

Control

a. Provide contingency training to system users consistent with assigned roles and responsibilities:

1. Within organizational policy defined timeframe (e.g. 1 month) of assuming a contingency role or responsibility;
2. When required by system changes; and
3. As per organizational policy (e.g. at least annually) thereafter; and

b. Review and update contingency training content as per organizational policy (e.g. annually) and following significant change.

Considerations

No additional OT clarification is required for this control.

CP-3(1) Contingency Training | Simulated Events

Implementation Level: 3

Control

Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.

Considerations

No additional OT clarification is required for this control.

CP-4 Contingency Plan Testing

Implementation Level: 1

Control

a. Test the contingency plan for the system in line with the requirements set in the Business Continuity Management System to determine the effectiveness of the plan and the readiness to execute the plan. Test options include but are not limited to: desktop walkthroughs; planned recovery of live data to a test environment; no-notice recovery of live data to a test environment.

b. Review the contingency plan test results; and

c. Initiate corrective actions, if needed.

Considerations

No additional OT clarification is required for this control.

CP-4(1) Contingency Plan Testing | Coordinate with Related Plans

Implementation Level: 2

Control Coordinate contingency plan testing with organizational elements responsible for related plans.

Considerations No additional OT clarification is required for this control.

CP-4(2) Contingency Plan Testing | Alternate Processing Site

Implementation Level 3

Control Test the contingency plan at the alternate processing site:

a. To familiarize contingency personnel with the facility and available resources; and

b. To evaluate the capabilities of the alternate processing site to support contingency operations.

Considerations Not all systems will have alternate processing sites, as discussed in CP-7.

CP-6 Alternate Storage Site

Implementation Level 2

Control a. Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and

b. Ensure that the alternate storage site provides controls equivalent to that of the primary site.

Considerations No additional OT clarification is required for this control.

CP-6(1) Alternate Storage Site | Separation from Primary Site

Implementation Level 2

Control Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.

Considerations No additional OT clarification is required for this control.

CP-6(2) Alternate Storage Site | Recovery Time and Recovery Point Objectives

Implementation Level 3

Control Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

Considerations No additional OT clarification is required for this control.

CP-6(3) Alternate Storage Site | Accessibility

Implementation Level 2

Control Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Considerations No additional OT clarification is required for this control.

CP-7 Alternate Processing Site

Implementation Level 2

Control a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of identified information system operations for essential mission and business functions within a time period consistent with recovery time and recovery point objectives when the primary processing capabilities are unavailable;

b. Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and

c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

Considerations Many site-wide supervisory or optimization servers (i.e. Level 3 and above of the Purdue model) can be supported from an alternate processing site. It is likely not feasible for control systems or field devices, such as sensors or final elements (i.e. Level 1 and 0 of the Purdue model), to be made available from an alternate processing site.

CP-7(1) Alternate Processing Site | Separation from Primary Site

Implementation Level 2

Control Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

Considerations No additional OT clarification is required for this control.

CP-7(2) Alternate Processing Site | Accessibility

Implementation Level **2**

Control Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Considerations No additional OT clarification is required for this control.

CP-7(3) Alternate Processing Site | Priority of Service

Implementation Level **2**

Control Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).

Considerations No additional OT clarification is required for this control.

CP-7(4) Alternate Processing Site | Preparation for Use

Implementation Level **3**

Control Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.

Considerations No additional OT clarification is required for this control.

CP-8 Telecommunications Services

Implementation Level **2**

Control Establish alternate telecommunications services, including necessary agreements to permit the resumption of defined system operations for essential mission and business functions within a defined time period in line with business requirements when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.

Considerations Quality of service factors for OT include latency and throughput.

CP-8(1) Telecommunications Services | Priority of Service Provisions

Implementation Level 2

Control a. Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and

b. Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.

Considerations No additional OT clarification is required for this control.

CP-8(2) Telecommunications Services | Single Points of Failure

Implementation Level 2

Control Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.

Considerations No additional OT clarification is required for this control.

CP-8(3) Telecommunications Services | Separation of Primary and Alternate Providers

Implementation Level 3

Control Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.

Considerations No additional OT clarification is required for this control.

CP-8(4) Telecommunications Services | Provider Contingency Plan

Implementation Level 3

Control a. Require primary and alternate telecommunications service providers to have contingency plans;

b. Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and

c. Obtain evidence of contingency testing and training by providers defined in contractual agreements and Service Level Agreement (SLA).

Considerations No additional OT clarification is required for this control.

CP-9 System Backup

Implementation Level 1

Control a. Conduct backups of user-level information contained in system components at a frequency consistent with recovery time and recovery point objectives;

b. Conduct backups of system-level information contained in the system at a frequency consistent with recovery time and recovery point objectives;

c. Conduct backups of system documentation, including security-related documentation at a frequency consistent with recovery time and recovery point objectives; and

d. Protect the confidentiality, integrity, and availability of backup information.

Considerations No additional OT clarification is required for this control.

CP-9(1) System Backup | Testing for Reliability and Integrity

Implementation Level 2

Control Test backup information to verify media reliability and information integrity:

a. In line with any legal, contractual, regulatory or other requirement;

b. As per organizational policy (e.g. at least annually) for Business Critical systems;

c. As per organizational policy (e.g. at least every 36 months) for non-Business Critical systems.

Considerations Testing for reliability and integrity increases confidence that the system can be restored after an incident and minimizes the impact associated with downtime and outages. The ability to test backups is often dependent on the resources needed to appropriately represent the environment, such as the availability of spare devices and testing equipment. Testing backup and restoration on OT is often limited to systems with redundancy or spare equipment. In certain cases, sampling will be limited to those redundant systems. Compensating controls may include alternative methods for testing backups, such as hash or checksum validations.

CP-9(2) System Backup | Test Restoration Using Sampling

Implementation Level 3

Control: Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.

Considerations: Testing for reliability and integrity increases confidence that the system can be restored after an incident and minimizes the impact associated with downtime and outages. The ability to test backups is often dependent on the resources needed to appropriately represent the environment, such as the availability of spare devices and testing equipment. Testing backup and restoration on OT is often limited to systems with redundancy or spare equipment. In certain cases, sampling will be limited to those redundant systems. Compensating controls may include alternative methods for testing backups, such as hash or checksum validations.

CP-9(3) System Backup | Separate Storage for Critical Information

Implementation Level 3

Control: Store backup copies of system components in a separate facility or in a fire rated container that is not collocated with the operational system.

Considerations: No additional OT clarification is required for this control.

CP-9(5) System Backup | Transfer to Alternate Storage Site

Implementation Level 3

Control: Transfer system backup information to the alternate storage site on a regular basis or at a frequency consistent with recovery time and recovery point objectives.

Considerations: No additional OT clarification is required for this control.

CP-9(8) System Backup | Cryptographic Protection

Implementation Level 2

Control Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of backup information for which this has been specified as a requirement.

Considerations No additional OT clarification is required for this control.

CP-10 System Recovery and Reconstitution

Implementation Level 1

Control Provide for the recovery and reconstitution of the system to a known state within a time period consistent with recovery time and recovery point objectives after a disruption, compromise, or failure.

Considerations Reconstitution of the OT includes considering whether system state variables should be restored to initial values or the values before disruption (e.g., are valves restored to full open, full closed, or settings prior to disruption). Restoring system state variables may be disruptive to ongoing physical processes (e.g., valves initially closed may adversely affect system cooling).

CP-10(2) System Recovery and Reconstitution | Transaction Recovery

Implementation Level 2

Control Implement transaction recovery for systems that are transaction-based.

Considerations No additional OT clarification is required for this control.

CP-10(4) System Recovery and Reconstitution | Restore Within Time Period

Implementation Level 3

Control Provide the capability to restore system components within defined recovery time and recovery point objectives from configuration-controlled and integrity-protected information representing a known, operational state for the components.

Considerations No additional OT clarification is required for this control.

CP-10(6) System Recovery and Reconstitution | Component Protection

Implementation Level 2

Control Protect system components used for recovery and reconstitution.

Considerations Organizations should consider recovery and reconstitution timeframes when storing spare equipment, including environmental hazards that could damage the equipment. Storage locations and environments should be chosen appropriately for the type of backup equipment.

OT system components stored without protection against environmental threats and unauthorized physical or logical access can be susceptible to compromise or damage. Certain system components may include embedded electronics that must be protected from environmental hazards.

CP-12 Safe Mode

Implementation Level 1

Control When certain conditions are detected, enter a safe mode of operation with defined restrictions of safe mode of operation.

Considerations No additional OT clarification is required for this control.

8 CONTROL FAMILY: IDENTIFICATION AND AUTHENTICATION

8.1 Control Implementation Levels

Control ID	Control | Control Enhancement	Implementation Level		
IA-1	**Policy and Procedures**	1		
IA-2	**Identification and Authentication (organizational Users)**	1		
IA-2(1)	Multi-factor Authentication to Privileged Accounts	1		
IA-2(2)	Multi-factor Authentication to Non-privileged Accounts		2	
IA-2(5)	Individual Authentication with Group Authentication			3
IA-2(6)	Access to Accounts —separate Device		2	
IA-2(8)	Access to Accounts — Replay Resistant			3
IA-3	**Device Identification and Authentication**		2	
IA-3(1)	Cryptographic Bidirectional Authentication		2	
IA-3(4)	Device Attestation		2	
IA-4	**Identifier Management**	1		
IA-4(4)	Identify User Status		2	
IA-5	**Authenticator Management**	1		
IA-5(1)	Password-based Authentication	1		
IA-5(2)	Public Key-based Authentication		2	
IA-5(6)	Protection of Authenticators		2	
IA-6	**Authentication Feedback**	1		
IA-7	**Cryptographic Module Authentication**	1		
IA-8	**Identification and Authentication (non-organizational Users)**	1		
IA-8(2)	Acceptance of External Authenticators			3
IA-8(4)	Use of Defined Profiles			3
IA-9	**Service Identification and Authentication**			3
IA-11	**Re-authentication**	1		
IA-12	**Identity Proofing**		2	
IA-12(1)	Supervisor Authorization			3
IA-12(2)	Identity Evidence		2	
IA-12(3)	Identity Evidence Validation and Verification		2	
IA-12(4)	In-person Validation and Verification			3
IA-12(5)	Address Confirmation		2	

8.2 Controls

IA-1 Policy and Procedures

Implementation Level: I

Control

a. Develop, document, and disseminate to appropriate personnel or roles:

1. An identification and authentication policy that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Is consistent with applicable laws, customer requirements, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;

b. Designate an individual to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and

c. Review and update the current identification and authentication:

1. Policy - e.g. annually and following significant change; and

2. Procedures - e.g. annually and following significant change.

Considerations

The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

IA-2 Identification and Authentication (organizational Users)

Implementation Level: I

Control

Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Considerations

When shared accounts are required, compensating controls include providing increased physical security, personnel security, and auditing measures. For certain OT, the capability for immediate operator interaction is critical. Local emergency actions for OT are not hampered by identification or authentication requirements. Access to these systems may be restricted by appropriate physical controls.

IA-2(1) Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts

Implementation Level 1

Control Implement multi-factor authentication for access to privileged accounts.

Considerations As a compensating control, physical access restrictions may sufficiently represent one authentication factor, provided that the system is not remotely accessible.

IA-2(2) Identification and Authentication (organizational Users) | Multi-factor Authentication to Non-privileged Accounts

Implementation Level 2

Control Implement multi-factor authentication for access to non-privileged accounts.

Considerations As a compensating control, physical access restrictions may sufficiently represent one authentication factor, provided that the system is not remotely accessible.

IA-2(5) Identification and Authentication (organizational Users) | Individual Authentication with Group Authentication

Implementation Level 3

Control When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.

Considerations For local access, physical access controls and logging may be used as an alternative to individual authentication on an OT system. For remote access, the remote access authentication mechanism will be used to identify, permit, and log individual access before permitting the use of shared accounts.

IA-2(6) Identification and Authentication (organizational Users) | Access to Accounts —separate Device

Implementation Level 2

Control Implement multi-factor authentication for local, network and remote access to privileged accounts and non-privileged accounts such that:

a. One of the factors is provided by a device separate from the system gaining access; and

b. The device meets strength of mechanism requirements approved by the Architecture Design Authority.

Considerations No additional OT clarification is required for this control.

IA-2(8) Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant

Implementation Level 3

Control Implement replay-resistant authentication mechanisms for access to privileged and non-privileged accounts.

Considerations No additional OT clarification is required for this control.

IA-3 Device Identification and Authentication

Implementation Level 2

Control Uniquely identify and authenticate the accessing device before establishing a network connection.

Considerations OT devices may not inherently support device authentication. If devices are local to one another, physical security measures that prevent unauthorized communication between devices can be used as compensating controls. For remote communication, additional hardware may be required to meet authentication requirements.

Given the variety of OT devices and physical locations of OT devices, organizations may consider whether OT devices that may be vulnerable to tampering or spoofing require unique identification and authentication and for what types of connections.

IA-3(1) Device Identification and Authentication | Cryptographic Bidirectional Authentication

Implementation Level 2

Control Authenticate devices before establishing a local, remote or network connection using bidirectional authentication that is cryptographically based.

Considerations For OT systems that include IIoT devices, these enhancements may be needed to protect device-to-device communication.

IA-3(4) Device Identification and Authentication | Device Attestation

Implementation Level 2

Control Handle device identification and authentication based on attestation by a configuration management process.

Considerations For OT systems that include IIoT devices, these enhancements may be needed to protect device-to-device communication.

IA-4 Identifier Management

Implementation Level 1

Control a. Receiving authorization from defined personnel or roles to assign an individual, group, role, service, or device identifier;

b. Selecting an identifier that identifies an individual, group, role, service, or device;

c. Assigning the identifier to the intended individual, group, role, service, or device; and

d. Preventing reuse of identifiers.

Considerations No additional OT clarification is required for this control.

IA-4(4) Identifier Management | Identify User Status

Implementation Level 2

Control Manage individual identifiers by uniquely identifying each individual as a member of a location, sub-organization of the Company or third party organisation as applicable.

Considerations This control enhancement is typically implemented by the organization rather than at the system level. However, to manage risk for certain OT environments, identifiers (e.g., badges) may have different markings to indicate the status of individuals, such as contractors, foreign nationals, and non-organizational users.

IA-5 Authenticator Management

Implementation Level 1

Control Manage system authenticators by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;

b. Establishing initial authenticator content for any authenticators issued by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;

e. Changing default authenticators prior to first use;

f. Changing or refreshing authenticators:

For individual accounts:

i) If network connected:

(1) Identity Access Management (IAM) joined Computer or user password as per organizational policy (e.g. at least 90 days),

(2) Not integrated with IAM Computer or user password as per organizational policy (e.g. at least annually).

ii) If standalone then:

(1) Computer or user password as per organizational policy (e.g. at least annually).

(2) Service or System accounts – as per organizational policy (e.g. annually),

(3) Hardware token - as per organizational policy (e.g. token lifetime),

Or for Group Accounts - when an individual leaves the group of authorized users;

g. Protecting authenticator content from unauthorized disclosure and modification;

h. Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and

i. Changing authenticators for group or role accounts when membership to those accounts changes.

Considerations

Example compensating controls include physical access control and encapsulating the OT to provide authentication external to the OT.

IA-5(1) Authenticator Management | Password-based Authentication

Implementation Level | I

Control

a. Maintain a list of commonly-used, expected, or compromised passwords and update the list as per organizational policy (e.g. monthly) and when organizational passwords are suspected to have been compromised directly or indirectly;

b. Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);

c. Transmit passwords only over cryptographically-protected channels;

d. Store passwords using an approved salted key derivation function, preferably using a keyed hash;

e. Require immediate selection of a new password upon account recovery;

f. Allow user selection of long passwords and passphrases, including spaces and all printable characters;

g. Employ automated tools to assist the user in selecting strong password authenticators; and

h. Enforce the following composition and complexity rules:

1. Passwords shall consist respective characters as defined in organizational policy (e.g. upper-case alphabetic; lower-case alphabetic; numeric; special characters, etc.).

2. Minimum length shall be as per organizational policy (e.g. Normal accounts - 12 characters, Privileged accounts (Developer or Local Admin) – 15 characters, Service Accounts – 15 characters, Highly privileged accounts (e.g. Root; Domain Administrator) – 20 characters).

3. Passwords cannot be the same password used the last 2–3 times before.

4. Password cannot contain first name and last name or the same spelling as the username.

Considerations No additional OT clarification is required for this control.

IA-5(2) Authenticator Management | Public Key-based Authentication

Implementation Level 2

Control a. For public key-based authentication:

1. Enforce authorized access to the corresponding private key; and

2. Map the authenticated identity to the account of the individual or group; and

b. When public key infrastructure (PKI) is used:

1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and

2. Implement a local cache of revocation data to support path discovery and validation.

Considerations No additional OT clarification is required for this control.

IA-5(6) Authenticator Management | Protection of Authenticators

Implementation Level 2

Control Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

Considerations No additional OT clarification is required for this control.

IA-6 Authentication Feedback

Implementation Level **1**

Control Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

Considerations This control assumes a visual interface that provides feedback about authentication information during the authentication process. When OT authentication uses an interface that does not support visual feedback (e.g., protocol-based authentication), this control may be tailored out.

IA-7 Cryptographic Module Authentication

Implementation Level **1**

Control Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, customer requirements, directives, policies, regulations, standards, and guidelines for such authentication.

Considerations No additional OT clarification is required for this control.

IA-8 Identification and Authentication (non-organizational Users)

Implementation Level **1**

Control Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

Considerations The Consideration for IA-2, Identification and Authentication (Organizational Users) is applicable for non-organizational users.

IA-8(2) Identification and Authentication (non-organizational Users) | Acceptance of External Authenticators

Implementation Level **3**

Control a. Accept only external authenticators that are organizational and Government compliant; and

b. Document and maintain a list of accepted external authenticators.

Considerations Example compensating controls include implementing support external to the OT and multi-factor authentication.

IA-8(4) Identification and Authentication (non-organizational Users) | Use of Defined Profiles

Implementation Level 3

Control Conform to the following profiles for identity management – use internal Company standard for Identification and authorization.

Considerations Example compensating controls include implementing support external to the OT and multi-factor authentication.

IA-9 Service Identification and Authentication

Implementation Level 3

Control Uniquely identify and authenticate critical systems and components before establishing communications with devices, users, or other services or applications.

Considerations No additional OT clarification is required for this control.

IA-11 Re-authentication

Implementation Level 1

Control Require users to re-authenticate when accounts are locked due to inactivity.

Considerations No additional OT clarification is required for this control.

IA-12 Identity Proofing

Implementation Level 2

Control

a. Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines;

b. Resolve user identities to a unique individual; and

c. Collect, validate, and verify identity evidence.

Considerations

Identity proofing is likely performed by different departments within the organization. Existing organizational systems (e.g., HR or IT processes) should be leveraged to perform this control.

IA-12(1) Identity Proofing | Supervisor Authorization

Implementation Level 3

Control

Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.

Considerations

Maintenance, engineering, or third-party organizations may require OT access in order to support operations. The organization should determine the AO for proving identity prior to allowing access to the OT environment. Consider obtaining supervisor or sponsor authorization, where the sponsor may be someone within operations.

A supervisor or sponsor should be made aware of any access that an employee has to the OT environment since unauthorized or accidental access could affect the physical process.

IA-12(2) Identity Proofing | Identity Evidence

Implementation Level 2

Control

Require evidence of individual identification be presented to the registration authority.

Considerations

If the organization already performs these controls, existing organizational processes should be leveraged. For example, HR may provide a system for tracking identity evidence. OT does not need to develop an independent system for achieving this control.

IA-12(3) Identity Proofing | Identity Evidence Validation and Verification

Implementation Level 2

Control Require that the presented identity evidence be validated and verified through a defined and auditable method.

Considerations If the organization already performs these controls, existing organizational processes should be leveraged. For example, HR may provide a system for tracking identity evidence. OT does not need to develop an independent system for achieving this control.

IA-12(4) Identity Proofing | In-person Validation and Verification

Implementation Level 3

Control Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.

Considerations If the organization already performs these controls, existing organizational processes should be leveraged. For example, HR may provide a system for tracking identity evidence. OT does not need to develop an independent system for achieving this control.

IA-12(5) Identity Proofing | Address Confirmation

Implementation Level 2

Control Require that a notice of proofing be delivered through an out-of-band channel to verify the users address (physical or digital) of record.

Considerations If the organization already performs these controls, existing organizational processes should be leveraged. For example, HR may provide a system for tracking identity evidence. OT does not need to develop an independent system for achieving this control.

9 CONTROL FAMILY: INCIDENT RESPONSE

9.1 Control Implementation Levels

Control ID	Control | Control Enhancement	Implementation Level		
IR-1	**Policy and Procedures**	1		
IR-2	**Incident Response Training**	1		
IR-2(1)	Simulated Events			3
IR-2(2)	Automated Training Environments			3
IR-2(3)	Breach	1		
IR-3	**Incident Response Testing**		2	
IR-3(2)	Coordination with Related Plans		2	
IR-4	**Incident Handling**	1		
IR-4(1)	Automated Incident Handling Processes		2	
IR-4(4)	Information Correlation			3
IR-4(11)	Integrated Incident Response Team			3
IR-5	**Incident Monitoring**	1		
IR-5(1)	Automated Tracking, Data Collection, and Analysis			3
IR-6	**Incident Reporting**	1		
IR-6(1)	Automated Reporting			2
IR-6(3)	Supply Chain Coordination			2
IR-7	**Incident Response Assistance**	1		
IR-7(1)	Automation Support for Availability of Information and Support			2
IR-8	**Incident Response Plan**	1		

9.2 Controls

IR-1 Policy and Procedures

Implementation Level 1

Control a. Develop, document, and disseminate to appropriate personnel or roles:

1. An incident response policy that:

   a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Is consistent with applicable laws, customer requirements, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;

b. Designate an individual to manage the development, documentation, and dissemination of the incident response policy and procedures; and

c. Review and update the current incident response:

1. As defined in organizational policy (e.g. every 2 years) or following significant change; and

2. Procedures as per organizational policy (e.g. annually) and following significant change.

Considerations The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

IR-2 Incident Response Training

Implementation Level 1

Control a. Provide incident response training to system users consistent with assigned roles and responsibilities:

1. As defined in organizational policy (e.g. within one month) of assuming an incident response role or responsibility or acquiring system access;

2. When required by system changes; and

3. As per organizational policy (e.g. at least annually) thereafter; and

b. Review and update incident response training content as defined in organizational policy (e.g. annually) and following a significant change.

Considerations No additional OT clarification is required for this control.

IR-2(1) Incident Response Training | Simulated Events

Implementation Level 3

Control Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.

Considerations No additional OT clarification is required for this control.

IR-2(2) Incident Response Training | Automated Training Environments

Implementation Level 3

Control Provide an incident response training environment using virtual training environment, attack simulation or Incident response platform.

Considerations No additional OT clarification is required for this control.

IR-2(3) Incident Response Training | Breach

Implementation Level 1

Control Provide incident response training on how to identify and respond to a breach, including the organization’s process for reporting a breach.

Considerations No additional OT clarification is required for this control.

IR-3 Incident Response Testing

Implementation Level 2

Control Test the effectiveness of the incident response capability for the system regulalry (e.g. at least annually) using the following tests: tabletop exercises and/or test invocations.

Considerations No additional OT clarification is required for this control.

IR-3(2) Incident Response Testing | Coordination with Related Plans

Implementation Level 2

Control Coordinate incident response testing with organizational elements responsible for related plans.

Considerations No additional OT clarification is required for this control.

IR-4 Incident Handling

Implementation Level 1

Control

a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinate incident handling activities with contingency planning activities;

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

d. Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

Considerations

As part of the incident handling capability, the organization coordinates with external vendors, integrators, or suppliers as necessary to ensure that they have the capability to address events that are specific to embedded components and devices.

IR-4(1) Incident Handling | Automated Incident Handling Processes

Implementation Level 2

Control

Support the incident handling process using automated mechanisms.

Considerations

No additional OT clarification is required for this control.

IR-4(4) Incident Handling | Information Correlation

Implementation Level 3

Control

Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

Considerations

No additional OT clarification is required for this control.

IR-4(11) Incident Handling | Integrated Incident Response Team

Implementation Level 3

Control

Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization Incident Response plan.

Considerations No additional OT clarification is required for this control.

IR-5 Incident Monitoring

Implementation Level 1

Control Track and document incidents.

Considerations No additional OT clarification is required for this control.

IR-5(1) Incident Monitoring | Automated Tracking, Data Collection, and Analysis

Implementation Level 3

Control Track incidents and collect and analyze incident information using Security Operation Centre metrics and root cause analysis.

Considerations No additional OT clarification is required for this control.

IR-6 Incident Reporting

Implementation Level 1

Control a. Require personnel to report suspected incidents to the organizational incident response capability immediately; and

b. Report incident information to organizations detailed in the incident response plan.

Considerations The organization should report incidents on a timely basis. NCSC-JO collaborates with international and private-sector computer emergency response teams (CERTs) to share control systems-related security incidents and mitigation measures.

IR-6(1) Incident Reporting | Automated Reporting

Implementation Level 2

Control Report incidents using automated mechanisms.

Considerations The automated mechanisms used to support the incident reporting process are not necessarily part of or connected to the OT.

IR-6(3) Incident Reporting | Supply Chain Coordination

Implementation Level 2

Control Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.

Considerations No additional OT clarification is required for this control.

IR-7 Incident Response Assistance

Implementation Level 1

Control Provide an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the system for the handling and reporting of incidents.

Considerations No additional OT clarification is required for this control.

IR-7(1) Incident Response Assistance | Automation Support for Availability of Information and Support

Implementation Level 2

Control Increase the availability of incident response information and support using automated mechanisms.

Considerations No additional OT clarification is required for this control.

IR-8 Incident Response Plan

Implementation Level I

Control

a. Develop an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall organization;
4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the organization;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;
8. Addresses the sharing of incident information;
9. Is reviewed and approved by the the Head of Cyber Security for the Sector, their designate, or Chief Information Security Officer (CISO) regularly (e.g. on at least an annual basis); and
10. Explicitly designates responsibility for incident response to appropriate personnel, or roles.

b. Distribute copies of the incident response plan to incident response personnel and appropriate organizational elements;

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;

d. Communicate incident response plan changes to incident response personnel and organizational elements; and

e. Protect the incident response plan from unauthorized disclosure and modification.

Considerations

No additional OT clarification is required for this control.

10 CONTROL FAMILY: MAINTENANCE

10.1 Control Implementation Levels

Control ID	Control | Control Enhancement	Implementation Level		
MA-1	**Policy and Procedures**	1		
MA-2	**Controlled Maintenance**	1		
MA-2(2)	Automated Maintenance Activities			3
MA-3	**Maintenance Tools**		2	
MA-3(1)	Inspect Tools		2	
MA-3(2)	Inspect Media		2	
MA-3(3)	Prevent Unauthorized Removal		2	
MA-4	**Nonlocal Maintenance**	1		
MA-4(1)	Logging and Review		2	
MA-4(3)	Comparable Security and Sanitization			3
MA-5	**Maintenance Personnel**	1		
MA-5(1)	Individuals Without Appropriate Access			3
MA-6	**Timely Maintenance**		2	

10.2 Controls

MA-1 Policy and Procedures

Implementation Level 1

Control

a. Develop, document, and disseminate to appropriate personnel or roles:

1. A system maintenance policy that:

    a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

    b. Is consistent with applicable laws, customer requirements, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;

b. Designate an individual to manage the development, documentation, and dissemination of the maintenance policy and procedures; and

c. Review and update the current maintenance:

1. As defined in organizational policy (e.g. every 2 years) and following

significant change; and

2. Procedures as per the organizational policy (e.g. every 2 years) and following significant change.

Considerations The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

MA-2 Controlled Maintenance

Implementation Level 1

Control a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;

c. Require that a Security Authority or their designate explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;

d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: Information detailed in Media Sanitization (MP-6) for sanitizing media and associated equipment.

e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and

f. Include the following information in organizational maintenance records: Appropriate information updated in organizational maintenance or asset registers.

Considerations No additional OT clarification is required for this control.

MA-2(2) *Optional* Controlled Maintenance | Automated Maintenance Activities

Implementation Level 3

Control a. Schedule, conduct, and document maintenance, repair, and replacement actions for the system using organizational maintenance or asset registers (ITSM); and

b. Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.

Considerations No additional OT clarification is required for this control.

MA-3 Maintenance Tools

Implementation Level **2**

Control a. Approve, control, and monitor the use of system maintenance tools; and
b. Review previously approved system maintenance tools regularly (e.g. at least annually).

Considerations No additional OT clarification is required for this control.

MA-3(1) Maintenance Tools | Inspect Tools

Implementation Level **2**

Control The organization inspects the maintenance tools carried into a facility by maintenance personnel for improper or unauthorized modifications.

Considerations No additional OT clarification is required for this control.

MA-3(2) Maintenance Tools | Inspect Media

Implementation Level **2**

Control Check media containing diagnostic and test programs for malicious code before the media are used in the system.

Considerations No additional OT clarification is required for this control.

MA-3(3) Maintenance Tools | Prevent Unauthorized Removal

Implementation Level **2**

Control Prevent the removal of maintenance equipment containing organizational information by:
a. Verifying that there is no organizational information contained on the equipment;
b. Sanitizing or destroying the equipment;
c. Retaining the equipment within the facility; or
d. Obtaining an exemption from the appropriate Head of Security/CISO explicitly authorizing removal of the equipment from the facility.

Considerations No additional OT clarification is required for this control.

MA-4 Nonlocal Maintenance

Implementation Level 1

Control a. Approve and monitor nonlocal maintenance and diagnostic activities;

b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;

c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;

d. Maintain records for nonlocal maintenance and diagnostic activities; and

f. Terminate session and network connections when nonlocal maintenance is completed.

Considerations No additional OT clarification is required for this control.

MA-4(1) Nonlocal Maintenance | Logging and Review

Implementation Level 2

Control a. Log audit events e.g. system event logs, alert logs, other maintenance logs for nonlocal maintenance and diagnostic sessions; and

b. Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.

Considerations No additional OT clarification is required for this control.

MA-4(3) Nonlocal Maintenance | Comparable Security and Sanitization

Implementation Level 3

Control a. Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or

b. Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.

Considerations The organization may need access to nonlocal maintenance and diagnostic services in order to restore essential OT operations or services. Example compensating controls include limiting the extent of the maintenance and diagnostic services to the minimum essential activities and carefully monitoring and auditing the nonlocal maintenance and diagnostic activities.

MA-5 Maintenance Personnel

Implementation Level 1

Control a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and

c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

Considerations No additional OT clarification is required for this control.

MA-5(1) Maintenance Personnel | Individuals Without Appropriate Access

Implementation Level 3

Control a. Implement procedures for the use of maintenance personnel that lack appropriate security clearances, that include the following requirements:

1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and
2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

b. Develop and implement additional layer of security including network segmentation, enhanced monitoring or access restrictions in the event a system component cannot be sanitized, removed, or disconnected from the system.

Considerations No additional OT clarification is required for this control.

MA-6 Timely Maintenance

Optional

Implementation Level 2

Control: Obtain maintenance support and/or spare parts for critical system components within an appropriate time period of failure.

Considerations: No additional OT clarification is required for this control.

11 CONTROL FAMILY: MEDIA PROTECTION

11.1 Control Implementation Levels

Control ID	Control | Control Enhancement	Implementation Level		
MP-1	**Policy and Procedures**	1		
MP-2	**Media Access**	1		
MP-3	**Media Marking**		2	
MP-4	**Media Storage**		2	
MP-5	**Media Transport**		2	
MP-6	**Media Sanitization**	1		
MP-6(1)	Review, Approve, Track, Document, and Verify			3
MP-6(2)	Equipment Testing			3
MP-6(3)	Nondestructive Techniques			3
MP-7	**Media Use**	1		

11.2 Controls

MP-1 Policy and Procedures

Implementation Level 1

Control a. Develop, document, and disseminate to appropriate personnel or roles:

1. A media protection policy that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Is consistent with applicable laws, customer requirements, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;

b. Designate an individual to manage the development, documentation, and dissemination of the media protection policy and procedures; and

c. Review and update the current media protection:

1. Policy - e.g. annually and following significant change; and

2. Procedures - e.g. annually and following significant change.

Considerations The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

MP-2 Media Access

Implementation Level 1

Control Restrict access to digital and non-digital media to authorized individuals or roles.

Considerations No additional OT clarification is required for this control.

MP-3 Media Marking

Implementation Level 2

Control Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.

Considerations No additional OT clarification is required for this control.

MP-4 Media Storage

Implementation Level 2

Control a. Physically control and securely store digital and non-digital media in line with any customer, contractual, company or legal requirements; and

b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Considerations No additional OT clarification is required for this control.

MP-5 Media Transport

Implementation Level 2

Control a. Protect and control digital and non-digital media during transport outside of controlled areas using controls specified within any customer, contractual, company or legal requirements;

b. Maintain accountability for system media during transport outside of controlled areas;

c. Document activities associated with the transport of system media; and

d. Restrict the activities associated with the transport of system media to authorized personnel.

Considerations No additional OT clarification is required for this control.

MP-6 Media Sanitization

Implementation Level 1

Control a. Sanitize all system media prior to disposal, release out of organizational control, or release for reuse using approved sanitization techniques and procedures; and

b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Considerations No additional OT clarification is required for this control.

MP-6(1) Media Sanitization | Review, Approve, Track, Document, and Verify

Implementation Level 3

Control Review, approve, track, document, and verify media sanitization and disposal actions.

Considerations No additional OT clarification is required for this control.

MP-6(2) Media Sanitization | Equipment Testing

Implementation Level 3

Control Test sanitization equipment and procedures regularly (e.g. at least annually) to ensure that the intended sanitization is being achieved.

Considerations No additional OT clarification is required for this control.

MP-6(3) Media Sanitization | Nondestructive Techniques

Implementation Level **3**

Control Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: portable storage devices used by third-party vendors or partners and devices used in highly sensitive areas.

Considerations No additional OT clarification is required for this control.

MP-7 Media Use

Implementation Level **1**

Control a. Restrict the use of system media on systems or system components using appropriate controls; and

b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

Considerations No additional OT clarification is required for this control.

12 CONTROL FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION

12.1 Control Implementation Levels

Control ID	Control | Control Enhancement	Implementation Level		
PE-2	**Physical Access Authorizations**	1		
PE-2(1)	Access by Position or Role	1		
PE-2(3)	Restrict Unescorted Access		2	
PE-3	**Physical Access Control**	1		
PE-3(1)	System Access			3
PE-4	**Access Control for Transmission**		2	
PE-5	**Access Control for Output Devices**		2	
PE-6	**Monitoring Physical Access**	1		
PE-6(1)	Intrusion Alarms and Surveillance Equipment		2	
PE-6(4)	Monitoring Physical Access to Systems			3
PE-8	**Visitor Access Records**	1		
PE-8(1)	Visitor Access Records | Automated Records Maintenance and Review			3
PE-9	**Power Equipment and Cabling**		2	
PE-10	**Emergency Shutoff**		2	
PE-11	**Emergency Power**		2	
PE-11(1)	Alternate Power Supply — Minimal Operational Capability			3
PE-12	**Emergency Lighting**	1		
PE-13	**Fire Protection**	1		
PE-13(1)	Detection Systems — Automatic Activation and Notification		2	
PE-13(2)	Suppression Systems — Automatic Activation and Notification			3
PE-14	**Environmental Controls**	1		
PE-15	**Water Damage Protection**	1		
PE-15(1)	Automation Support			3
PE-16	**Delivery and Removal**	1		
PE-17	**Alternate Work Site**			2
PE-18	**Location of System Components**			3
PE-20	**Asset Monitoring and Tracking**			3

12.2 Controls

PE-2 Physical Access Authorizations

Implementation Level: 1

Control

a. Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;

b. Issue authorization credentials for facility access;

c. Review the access list detailing authorized facility access by individuals regularly (e.g. quarterly); and

d. Remove individuals from the facility access list when access is no longer required.

Considerations

No additional OT clarification is required for this control.

PE-2(1) Physical Access Authorizations | Access by Position or Role

Implementation Level: 1

Control

Authorize physical access to the facility where the system resides based on position or role.

Considerations

No additional OT clarification is required for this control.

PE-2(3) Physical Access Authorizations | Restrict Unescorted Access

Implementation Level: 2

Control

Restrict unescorted access to the facility where the system resides to personnel with formal access authorizations for:

a. all information contained within the system; or

b. need for access to all information contained within the system;

Areas allowed will be defined by staff roles and visitors purpose.

Considerations

No additional OT clarification is required for this control.

PE-3 Physical Access Control

Optional

Implementation Level: 1

Control

a. Enforce physical access authorizations at entry and exit points to the facility where the system resides by:

1. Verifying individual access authorizations before granting access to the facility; and
2. Controlling ingress and egress to the facility using access card, biometric scanners or revolving doors and guards;

b. Maintain physical access audit logs for all personnel including employees and visitors;

c. Control access to areas within the facility designated as publicly accessible by implementing the following controls: sign visitors in log book; assign visitor passes with access restriction to publicly accessible areas only;

d. Escort visitors and control visitor activity at all times by authorized personnel;

e. Secure keys, combinations, and other physical access devices;

f. Inventory physical access devices as defined in organizational policy (e.g. monthly); and

g. Change combinations and keys regularly (e.g. annually) and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.

Considerations

No additional OT clarification is required for this control.

PE-3(1) Physical Access Control | System Access

Optional

Implementation Level: 3

Control

Enforce physical access authorizations to the system in addition to the physical access controls for the facility and physical spaces containing one or more components of the system:

a. PIN pads and Key Cards

b. MFA with Smart Cards or other devices

c. Role Based Access Control enforced access

d. Dynamic Authentication

Considerations

No additional OT clarification is required for this control.

PE-4 Access Control for Transmission

Implementation Level 2

Control: Control physical access to all facilities, equipment, systems, system components and personell within organizational facilities using organizational policies.

Considerations: No additional OT clarification is required for this control.

PE-5 Access Control for Output Devices

Implementation Level 2

Control: Control physical access to output from critical systems, system components and devices to prevent unauthorized individuals from obtaining the output.

Considerations: No additional OT clarification is required for this control.

PE-6 Monitoring Physical Access

Implementation Level 1

Control:

a. Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;

b. Review physical access logs as defined in organizational policy (e.g. weekly basis) and upon occurrence of reported incident; and

c. Coordinate results of reviews and investigations with the organizational incident response capability.

Considerations: No additional OT clarification is required for this control.

PE-6(1) *Optional* Monitoring Physical Access | Intrusion Alarms and Surveillance Equipment

Implementation Level 2

Control: Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.

Considerations: No additional OT clarification is required for this control.

PE-6(4) *Optional* — Monitoring Physical Access | Monitoring Physical Access to Systems

Implementation Level: 3

Control: Monitor physical access to the system in addition to the physical access monitoring of the facility at classified locations.

Considerations: No additional OT clarification is required for this control.

PE-8 — Visitor Access Records

Implementation Level: 1

Control:

a. Maintain visitor access records to the facility where the system resides as defined in organizational policy (e.g. for 1 year);

b. Review visitor access records on a regular basis; and

c. Report anomalies in visitor access records to physical security and Information security teams.

Considerations: No additional OT clarification is required for this control.

PE-8(1) — Visitor Access Records | Automated Records Maintenance and Review

Implementation Level: 3

Control: Maintain and review visitor access records using management access system on a regular basis (e.g. quarterly).

Considerations: No additional OT clarification is required for this control.

PE-9 *Optional* — Power Equipment and Cabling

Implementation Level: 2

Control: Protect power equipment and power cabling for the system from damage and destruction.

Considerations: No additional OT clarification is required for this control.

PE-10 Emergency Shutoff

Optional

Implementation Level 2

Control a. Provide the capability of shutting off power to critical systems or individual system components in emergency situations;

b. Place emergency shutoff switches or devices in entry location by system or system component to facilitate access for authorized personnel; and

c. Protect emergency power shutoff capability from unauthorized activation.

Considerations No additional OT clarification is required for this control.

PE-11 Emergency Power

Optional

Implementation Level 2

Control Provide an uninterruptible power supply to facilitate an orderly shutdown of the system; transition of the system to long-term alternate power in the event of a primary power source loss.

Considerations No additional OT clarification is required for this control.

PE-11(1) Emergency Power | Alternate Power Supply — Minimal Operational Capability

Implementation Level 3

Control Provide an alternate power supply for the system that is activated automatically and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.

Considerations No additional OT clarification is required for this control.

PE-12 Emergency Lighting

Optional

Implementation Level 1

Control Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Considerations No additional OT clarification is required for this control.

PE-13 Fire Protection

Optional

Implementation Level 1

Control Employ and maintain fire detection and suppression systems that are supported by an independent energy source.

Considerations No additional OT clarification is required for this control.

PE-13(1) Fire Protection | Detection Systems — Automatic Activation and Notification

Optional

Implementation Level 2

Control Employ fire detection systems that activate automatically and notify respective personnel, fire wardens and emergency responders in the event of a fire.

Considerations No additional OT clarification is required for this control.

PE-13(2) Fire Protection | Suppression Systems — Automatic Activation and Notification

Optional

Implementation Level 3

Control a. Employ fire suppression systems that activate automatically and notify facility manager and respective emergency responders; and

b. Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.

Considerations No additional OT clarification is required for this control.

PE-14 Environmental Controls

Optional

Implementation Level 1

Control a. Maintain temperature; humidity; and other required measurements as per environmental control levels within the facility where the system resides at manufacturer acceptable levels; and

b. Monitor environmental control levels on regular basis.

Considerations No additional OT clarification is required for this control.

PE-15 *Optional* Water Damage Protection

Implementation Level 1

Control Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Considerations No additional OT clarification is required for this control.

PE-15(1) *Optional* Water Damage Protection | Automation Support

Implementation Level 3

Control Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

Considerations No additional OT clarification is required for this control.

PE-16 Delivery and Removal

Implementation Level 1

Control a. Authorize and control critical system components entering and exiting the facility; and

b. Maintain records of the system components.

Considerations No additional OT clarification is required for this control.

PE-17 Alternate Work Site

Implementation Level 2

Control

a. Determine and document all alternate sites allowed for use by employees;

b. Employ the following controls at alternate work sites: IT and Network security controls, Operational controls, Physical controls;

c. Assess the effectiveness of controls at alternate work sites; and

d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

Considerations

No additional OT clarification is required for this control.

PE-18 Location of System Components

Optional

Implementation Level 3

Control

Position system components within the facility to minimize potential damage from damage or physical and environmental hazards and to minimize the opportunity for unauthorized access.

Considerations

No additional OT clarification is required for this control.

PE-20 Asset Monitoring and Tracking

Optional

Implementation Level 3

Control

Employ Radio Frequency Identification (RFID), Wi-Fi, GPS and other sensors to track and monitor the location and movement of critical assets and components in all facilities.

Considerations

No additional OT clarification is required for this control.

13 CONTROL FAMILY: PLANNING

13.1 Control Implementation Levels

Control ID	Control | Control Enhancement	Implementation Level		
PL-1	**Policy and Procedures**	1		
PL-2	**System Security and Privacy Plans**	1		
PL-4	**Rules of Behavior**	1		
PL-4(1)	Social Media and External Site/application Usage Restrictions		2	
PL-8	**Security and Privacy Architectures**		2	
PL-8(1)	Defense in Depth		2	
PL-10	**Baseline Selection**	1		
PL-11	**Baseline Tailoring**	1		

13.2 Controls

PL-1 Policy and Procedures

Implementation Level 1

Control

a. Develop, document, and disseminate to appropriate personnel or roles:

1. A planning policy that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Is consistent with applicable laws, customer requirements, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the planning policy and the associated planning controls;

b. Designate an individual to manage the development, documentation, and dissemination of the planning policy and procedures; and

c. Review and update the current planning:

1. Policy – e.g. annually and following significant change; and

2. Procedures – e.g. annually and following significant change.

Considerations

The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

PL-2 System Security and Privacy Plans

Implementation Level: I

Control a. Develop security plans for the system that:

1. Are consistent with the organization's enterprise architecture;
2. Explicitly define the constituent system components;
3. Describe the operational context of the system in terms of mission and business processes;
4. Identify the individuals that fulfill system roles and responsibilities;
5. Identify the information types processed, stored, and transmitted by the system;
6. Provide the security categorization of the system, including supporting rationale;
7. Describe any specific threats to the system that are of concern to the organization;
8. Provide the results of a privacy risk assessment for systems processing personally identifiable information;
9. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
10. Provide an overview of the security requirements for the system;
11. Identify any relevant control baselines or overlays, if applicable;
12. Describe the controls in place or planned for meeting the security requirements, including a rationale for any tailoring decisions;
13. Include risk determinations for security architecture and design decisions;
14. Include security-related activities affecting the system that require planning and coordination with relevant other parts of the organization; and
15. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

b. Distribute copies of the plans and communicate subsequent changes to the plans to appropriate personnel or roles;

c. Review the plans regulalry (e.g. annually) or following significant change;

d. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and

e. Protect the plans from unauthorized disclosure and modification.

Considerations When systems are highly interconnected, coordinated planning is essential. A low-impact system could adversely affect a higher-impact system.

PL-4 Rules of Behavior

Implementation Level: I

Control a. Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behaviour for information and system usage, and security;

b. Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behaviour, before authorizing access to information and the system;

c. Review and update the rules of behaviour regularly (e.g. annually); and

d. Require individuals who have acknowledged a previous version of the rules of behaviour to read and re-acknowledge when the rules are revised or updated.

Considerations No additional OT clarification is required for this control.

PL-4(1) Rules of Behavior | Social Media and External Site/application Usage Restrictions

Implementation Level 2

Control Include in the rules of behaviour, restrictions on:

a. Use of social media, social networking sites, and external sites/applications;

b. Posting organizational information on public websites; and

c. Use of organization-provided identifiers (e.g. email addresses) and authentication secrets (e.g. passwords) for creating accounts on external sites/applications.

Considerations No additional OT clarification is required for this control.

PL-8 Security and Privacy Architectures

Implementation Level 2

Control a. Develop security architectures for the system that:

1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;

2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;

3. Describe how the architectures are integrated into and support the enterprise architecture; and

4. Describe any assumptions about, and dependencies on, external systems and services;

b. Review and update the architectures regularly (e.g. annually) or following significant change to reflect changes in the enterprise architecture.

Considerations No additional OT clarification is required for this control.

PL-8(1) Security and Privacy Architectures | Defense in Depth

Implementation Level: 2

Control: Design the security and privacy architectures for the system using a defense-in-depth approach that:

a. Allocates organization-defined controls to locations and architectural layers; and

b. Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.

Considerations: Defense in depth is considered a common practice for security architecture within OT environments.

PL-10 Baseline Selection

Implementation Level: 1

Control: Select a control baseline for the system.

Considerations: No additional OT clarification is required for this control.

PL-11 Baseline Tailoring

Implementation Level: 1

Control: Tailor the selected control baseline by applying specified tailoring actions.

Considerations: No additional OT clarification is required for this control.

14 CONTROL FAMILY: RISK ASSESSMENT

14.1 Control Implementation Levels

Control ID	Control | Control Enhancement	Implementation Level		
RA-1	**Policy and Procedures**	1		
RA-2	**Security Categorization**	1		
RA-3	**Risk Assessment**	1		
RA-3(1)	Supply Chain Risk Assessment	1		
RA-5	**Vulnerability Monitoring and Scanning**	1		
RA-5(2)	Update Vulnerabilities to Be Scanned	1		
RA-5(4)	Discoverable Information			3
RA-5(5)	Privileged Access		2	
RA-5(11)	Public Disclosure Program		2	
RA-7	**Risk Response**	1		
RA-9	**Criticality Analysis**		2	

14.2 Controls

RA-1 Policy and Procedures

Implementation Level 1

Control a. Develop, document, and disseminate to appropriate personnel or roles:

1. A risk assessment policy that:
    a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    b. Is consistent with applicable laws, customer requirements, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

b. Designate an individual to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and

c. Review and update the current risk assessment:

1. Policy – e.g. annually and following significant change; and
2. Procedures – e.g. annually and following significant change.

Considerations The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

RA-2 Security Categorization

Implementation Level I

Control a. Categorize the system and information it processes, stores, and transmits;

b. Document the security categorization results, including supporting rationale, in the security plan for the system; and

c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.

Considerations PHA, functional safety assessments, and other organization-established risk assessments can be referenced to identify the impact level of the OT systems.

RA-3 Risk Assessment

Implementation Level I

Control a. Conduct a risk assessment, including:

1. Identifying threats to and vulnerabilities in the system;
2. Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
3. Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

b. Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;

c. Document risk assessment results in in accordance with local working practices, e.g. local risk register or Risk and Compliance tool;

d. Review risk assessment results as defined in organizational policy (e.g. at least every 6 months);

e. Disseminate risk assessment results to relevant parties; and

f. Update the risk assessment as defined in organizational policy (e.g. annually) or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security state of the system.

Considerations No additional OT clarification is required for this control.

RA-3(1) Risk Assessment | Supply Chain Risk Assessment

Implementation Level | I

Control

a. Assess supply chain risks associated with systems, system components, and system services; and

b. Update the supply chain risk assessment regularly (e.g. annually) or when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.

Considerations

No additional OT clarification is required for this control.

RA-5 Vulnerability Monitoring and Scanning

Implementation Level | I

Control

a. Monitor and scan for vulnerabilities in the system and hosted applications outlined in company Vulnerability Management Policy and when new vulnerabilities potentially affecting the system are identified and reported;

b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

1. Enumerating platforms, software flaws, and improper configurations;
2. Formatting checklists and test procedures; and
3. Measuring vulnerability impact.

c. Analyse vulnerability scan reports and results from vulnerability monitoring;

d. Remediate legitimate vulnerabilities or implement approved compensating controls within a timeframe dependent upon criticality of the vulnerabilities and agreed upon between the Information Security (or delegate) and the information system owner in accordance with an organizational assessment of risk;

e. Share information obtained from the vulnerability monitoring process and control assessments with Systems Administrators to help eliminate similar vulnerabilities in other systems; and

f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

Considerations

The organization makes a risk-based determination of how to monitor or scan for vulnerabilities on their system. This may include active scanning, passive monitoring, or compensating controls, depending on the system being scanned. For example, vulnerability examination may be performed using passive monitoring and manual visual inspection to maintain an up-to-date inventory of assets. That inventory can be cross-referenced against a list of known vulnerabilities (e.g., NCSC-JO advisories, NIST NVD). Production may need to be taken offline before active scans can be conducted. Scans are scheduled to occur during planned IT/OT outages whenever possible. If vulnerability scanning tools are used on adjacent non-OT networks, extra care is taken to ensure that they do not mistakenly scan the IT/OT network.

Automated network scanning is not applicable to non-routable communications, such as serial networks. Compensating controls include providing a replicated or simulated system for conducting scans or host-based vulnerability applications.

RA-5(2) Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanned

Implementation Level 1

Control Update the system vulnerabilities to be scanned regularly (e.g. weekly); prior to a new scan; or when new vulnerabilities are identified and reported.

Considerations No additional OT clarification is required for this control.

RA-5(4) Vulnerability Monitoring and Scanning | Discoverable Information

Implementation Level 3

Control Determine information about the system that is discoverable and take actions to secure the components by hardening system configuration, applying segmentation, restricting access where possible and perform continues security monitoring.

Considerations Examples of discoverable information in OT could include information about key personnel or technical information related to systems and configurations. Locations that may need to be monitored or scanned include technical forums, blogs, and vendor or contractor websites.

RA-5(5) Vulnerability Monitoring and Scanning | Privileged Access

Implementation Level 2

Control Implement privileged access authorization to selected system components for vulnerability scanning activities.

Considerations No additional OT clarification is required for this control.

RA-5(11) Vulnerability Monitoring and Scanning | Public Disclosure Program

Implementation Level 2

Control Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

Considerations CNI organizations,may have to develop and publish a vulnerability disclosure policy for their internet-accessible systems and services and maintain processes to support it. A vulnerability disclosure policy may be implemented at the organization level rather than for each system.CNI organizations could achieve this control by creating and monitoring an email address published on a public-facing website for contacting the organization regarding disclosures.

RA-7 Risk Response

Implementation Level 1

Control Respond to findings from security assessments, monitoring, and audits in accordance with organizational risk tolerance.

Considerations No additional OT clarification is required for this control.

RA-9 Criticality Analysis

Implementation Level 2

Control Identify critical system components and functions by performing a criticality analysis for systems, system components, or system services at appropriate decision points in the system development life cycle.

Considerations No additional OT clarification is required for this control.

15 CONTROL FAMILY: SYSTEM AND SERVICES ACQUISITION

15.1 Control Implementation Levels

Control ID	Control | Control Enhancement	Implementation Level		
SA-1	**Policy and Procedures**	1		
SA-2	**Allocation of Resources**	1		
SA-3	**System Development Life Cycle**	1		
SA-3(1)	Manage Preproduction Environment	1		
SA-3(2)	Use of Live or Operational Data			3
SA-3(3)	Technology Refresh	1		
SA-4	**Acquisition Process**	1		
SA-4(1)	Functional Properties of Controls		2	
SA-4(2)	Design and Implementation Information for Controls		2	
SA-4(5)	System, Component, and Service Configurations			3
SA-4(9)	Functions, Ports, Protocols, and Services in Use		2	
SA-4(12)	Data Ownership	1		
SA-5	**System Documentation**	1		
SA-8	Security **and Privacy Engineering Principles**	1		
SA-9	**External System Services**	1		
SA-9(2)	Identification of Functions, Ports, Protocols, and Services		2	
SA-10	**Developer Configuration Management**		2	
SA-11	**Developer Testing and Evaluation**		2	
SA-15	**Development Process, Standards, and Tools**		2	
SA-15(3)	Criticality Analysis		2	
SA-16	**Developer-provided Training**			3
SA-17	**Developer Security and Privacy Architecture and Design**			3
SA-21	**Developer Screening**			3
SA-22	**Unsupported System Components**	1		

15.2 Controls

SA-1 Policy and Procedures

Implementation Level 1

Control

a. Develop, document, and disseminate to appropriate personnel or roles:

1. A system and services acquisition policy that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Is consistent with applicable laws, customer requirements, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls.

b. Designate an individual to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and

c. Review and update the current system and services acquisition:

1. Policy – e.g. annually and following significant change; and

2. Procedures – e.g. annually and following significant change.

Considerations

The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

SA-2 Allocation of Resources

Implementation Level 1

Control

a. Determine the high-level information security requirements for the system or system service in mission and business process planning;

b. Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and

c. Establish a discrete line item for information security in organizational programming and budgeting documentation.

Considerations

No additional OT clarification is required for this control.

SA-3 System Development Life Cycle

Implementation Level: 1

Control

a. Acquire, develop, and manage the system using a Business Unit approved System Development approach that incorporates information security considerations;

b. Define and document information security roles and responsibilities throughout the system development life cycle;

c. Identify individuals having information security roles and responsibilities; and

d. Integrate the organizational information security risk management process into system development life cycle activities.

Considerations

No additional OT clarification is required for this control.

SA-3(1) System Development Life Cycle | Manage Preproduction Environment

Implementation Level: 1

Control

Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.

Considerations

Organizations that do not maintain local pre- production environments and utilize a third-party integrator should ensure that contracts are developed to limit security and privacy risks.

SA-3(2) System Development Life Cycle | Use of Live or Operational Data

Implementation Level: 3

Control

a. Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service; and

b. Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments.

Considerations

No additional OT clarification is required for this control.

SA-3(3) System Development Life Cycle | Technology Refresh

Implementation Level: 1

Control

Plan for and implement a technology refresh schedule where possible for the system throughout the system development life cycle.

Considerations Many OT systems have an expected life cycle that is longer than most IT components. Technology refresh is addressed in budget planning to limit the use of obsolete systems that present security or reliability risks.

SA-4 Acquisition Process

Implementation Level 1

Control Include the following requirements, descriptions, and criteria, explicitly or by reference, using standardized contract language in the acquisition contract for the system, system component, or system service:

a. Security functional requirements;

b. Strength of mechanism requirements;

c. Security assurance requirements;

d. Controls needed to satisfy the security requirements.

e. Security documentation requirements;

f. Requirements for protecting security documentation;

g. Description of the system development environment and environment in which the system is intended to operate;

h. Allocation of responsibility or identification of parties responsible for information security and supply chain risk management; and

i. Acceptance criteria.

Considerations Organizations engage with OT suppliers to raise awareness of cybersecurity needs.

SA-4(1) Acquisition Process | Functional Properties of Controls

Implementation Level 2

Control Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.

Considerations When acquiring OT products, consideration for security requirements may not have been incorporated into the design. Procurement may need to consider alternative products or complementary hardware or plan for compensating controls.

SA-4(2) Acquisition Process | Design and Implementation Information for Controls

Implementation Level **2**

Control: Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes appropriate elements such as: Solution definition; security-relevant external system interfaces; high-level design; low-level design; application architecture – including data flow; hardware schematics; at an appropriate level of detail to enable a technical design review of security controls to be completed.

Considerations: When acquiring OT products, consideration for security requirements may not have been incorporated into the design. Procurement may need to consider alternative products or complementary hardware or plan for compensating controls.

SA-4(5) Acquisition Process | System, Component, and Service Configurations

Implementation Level **3**

Control: Require the developer of the system, system component, or system service to:

a. Deliver the system, component, or service with predifned and agreed secure configurations implemented; and

b. Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.

Considerations: No additional OT clarification is required for this control.

SA-4(9) Acquisition Process | Functions, Ports, Protocols, and Services in Use

Implementation Level **2**

Control: Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.

Considerations: When acquiring OT products, consideration for security requirements may not have been incorporated into the design. Procurement may need to consider alternative products or complementary hardware or plan for compensating controls.

SA-4(12) Acquisition Process | Data Ownership

Implementation Level I

Control a. Include organizational data ownership requirements in the acquisition contract; and

b. Require all data to be removed from the contractor's system and returned to the organization as defined in organizational policy (e.g. within 30 days).

Considerations No additional OT clarification is required for this control.

SA-5 System Documentation

Implementation Level I

Control a. Obtain or develop administrator documentation for the system, system component, or system service that describes:

1. Secure configuration, installation, and operation of the system, component, or service;
2. Effective use and maintenance of security functions and mechanisms; and
3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

b. Obtain or develop user documentation for the system, system component, or system service that describes:

1. User-accessible security functions and mechanisms and how to effectively use those functions and mechanisms;
2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and
3. User responsibilities in maintaining the security of the system, component, or service;

c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and where required, generate suitable supporting documentation in-house in response; and

d. Distribute documentation to appropriate personnel or roles.

Considerations No additional OT clarification is required for this control.

SA-8 Security and Privacy Engineering Principles

Implementation Level I

Control Apply the following systems security engineering principles in the specification, design, development, implementation, and modification of the system and system components: Appropriate elements of security engineering principles incorporated in systems development activities. The principles employed will depend upon the nature and scale of the system being developed or upgraded.

Considerations No additional OT clarification is required for this control.

SA-9 External System Services

Implementation Level 1

Control a. Require that providers of external system services comply with organizational security requirements and employ the following controls: the Organizational process specifies mandatory requirements for external system services.

b. Define and document organizational oversight and user roles and responsibilities with regard to external system services; and

c. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: As per the organizational process, the responsibility for ensuring appropriate controls are in place and working effectively rests with the system or service owner.

Considerations No additional OT clarification is required for this control.

SA-9(2) External System Services | Identification of Functions, Ports, Protocols, and Services

Implementation Level 2

Control Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: Any external system or service.

Considerations No additional OT clarification is required for this control.

SA-10 Developer Configuration Management

Implementation Level 2

Control Require the developer of the system, system component, or system service to:

a. Perform configuration management during system, component, or service design; development; implementation; operation; disposal;

b. Document, manage, and control the integrity of changes to configuration items under configuration management;

c. Implement only organization-approved changes to the system, component, or service;

d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and

e. Track security flaws and flaw resolution within the system, component, or service and report findings to appropriate personnel or roles.

Considerations Personnel with knowledge about security and privacy requirements are included in the change management process for the developer.

SA-11 Developer Testing and Evaluation

Implementation Level 2

Control Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

a. Develop and implement a plan for ongoing security control assessments;

b. Perform appropriate testing/evaluation when required. Examples of testing include unit; integration; system; regression testing;

c. Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;

Considerations No additional OT clarification is required for this control.

SA-15 Development Process, Standards, and Tools

Implementation Level 2

Control a. Require the developer of the system, system component, or system service to follow a documented development process that:

1. Explicitly addresses security requirements;
2. Identifies the standards and tools used in the development process;
3. Documents the specific tool options and tool configurations used in the development process; and
4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

b. Review the development process, standards, tools, tool options, and tool configurations annually to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security requirements:

1. Protective monitoring (with use cases defined for application monitoring),
2. Enterprise AV / Anti Malware Protection.
3. Vulnerability Scanning.
4. No Obsolescence (products are vendor supported and have not gone beyond N-1 in their lifecycle; where N is the latest version available).

5. Update / Patch Scheduling are defined.

Considerations	No additional OT clarification is required for this control.

SA-15(3) Development Process, Standards, and Tools | Criticality Analysis

Implementation Level **2**

Control	Require the developer of the system, system component, or system service to perform a criticality analysis: a. At the following decision points in the system development life cycle: At all stages of development from solution definition onwards; and b. At the following level of rigor: At an appropriate level of detail to enable a Technical Design Review of security controls to be performed.
Considerations	No additional OT clarification is required for this control.

SA-16 Developer-provided Training

Implementation Level **3**

Control	Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: Virtual or in-person vendor training.
Considerations	No additional OT clarification is required for this control.

SA-17 Developer Security and Privacy Architecture and Design

Implementation Level **3**

Control	Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that: a. Is consistent with the organization’s security and privacy architecture that is an integral part the organization’s enterprise architecture; b. Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and c. Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.

Considerations No additional OT clarification is required for this control.

SA-21 Developer Screening

Implementation Level 3

Control Require that the developer of system component or system service:

a. Has appropriate access authorizations as determined by assigned role ; and

b. Satisfies the following additional personnel screening criteria: background checks, security clearance and security screening.

Considerations No additional OT clarification is required for this control.

SA-22 Unsupported System Components

Implementation Level 1

Control a. Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or

b. Provide one or more of the following options for alternative sources for continued support for unsupported components: In-house support; support from external providers; extended custom support from OEM; deployment of protective hardware or software.

Considerations OT systems may contain system components that are no longer supported by the developer, vendor, or manufacturer and have not been replaced due to various operational, safety, availability, or lifetime constraints. Organizations identify alternative methods to continue supported operation of such system components and consider additional compensating controls to mitigate against known threats and vulnerabilities to unsupported system components.

16 CONTROL FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION

16.1 Control Implementation Levels

Control ID	Control | Control Enhancement	Implementation Level		
SC-1	**Policy and Procedures**	1		
SC-2	**Separation of System and User Functionality**		2	
SC-3	**Security Function Isolation**			3
SC-4	**Information in Shared System Resources**		2	
SC-5	**Denial-of-service Protection**	1		
SC-7	**Boundary Protection**	1		
SC-7(3)	Access Points		2	
SC-7(4)	External Telecommunications Services		2	
SC-7(5)	Deny by Default — Allow by Exception		2	
SC-7(7)	Split Tunneling for Remote Devices		2	
SC-7(8)	Route Traffic to Authenticated Proxy Servers		2	
SC-7(16)	Prevent Discovery of System Components		2	
SC-7(18)	Fail Secure			3
SC-7(21)	Isolation of System Components			3
SC-7(28)	Connections to Public Networks	1		
SC-7(29)	Separate Subnets to Isolate Functions		2	
SC-8	**Transmission Confidentiality and Integrity**		2	
SC-8(1)	**Transmission Confidentiality and Integrity | Cryptographic Protection**		2	
SC-12	**Cryptographic Key Establishment and Management**	1		
SC-12(1)	Availability			3
SC-13	**Cryptographic Protection**	1		
SC-15	**Collaborative Computing Devices and Applications**	1		
SC-17	**Public Key Infrastructure Certificates**		2	
SC-18	**Mobile Code**		2	
SC-20	**Secure Name/address Resolution Service (authoritative Source)**	1		
SC-21	**Secure Name/address Resolution Service (recursive or Caching Resolver)**	1		
SC-22	**Architecture and Provisioning for Name/address Resolution Service**	1		
SC-23	**Session Authenticity**		2	
SC-24	**Fail in Known State**			3

Control ID	Control | Control Enhancement	Implementation Level		
SC-28	**Protection of Information at Rest**		2	
SC-28(1)	Cryptographic Protection		2	
SC-29	**Heterogeneity**		2	
SC-30	**Concealment and Misdirection**			3
SC-31	**Covert Channel Analysis**			3
SC-39	**Process Isolation**	1		
SC-41	**Port and I/O Device Access**		2	
SC-44	**Detonation Chambers**			3
SC-45	**System Time Synchronization**	1		
SC-45(1)	Synchronization with Authoritative Time Source	1		

16.2 Controls

SC-1 Policy and Procedures

Implementation Level 1

Control a. Develop, document, and disseminate to appropriate personnel or roles:

1. A system and communications protection policy that:

   a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

   b. Is consistent with applicable laws, customer requirements, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;

b. Designate an Individual to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and

c. Review and update the current system and communications protection:

1. Policy – e.g. annually and following significant change; and
2. Procedures – e.g. annually and following significant change.

Considerations The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

SC-2 Separation of System and User Functionality

Implementation Level 2

Control Separate user functionality, including user interface services, from system management functionality.

Considerations Physical separation includes using separate systems for managing the OT and for operating OT components. Logical separation includes the use of different user accounts for administrative and operator privileges. Example compensating controls include providing increased auditing measures.

SC-3 Security Function Isolation

Implementation Level 3

Control Isolate security functions from nonsecurity functions.

Considerations Organizations consider implementing this control when designing new architectures or updating existing components. An example compensating control includes access controls.

SC-4 Information in Shared System Resources

Implementation Level 2

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

Considerations This control is especially relevant for OT systems that process confidential data. Example compensating controls include engineering the use of the OT to prevent sharing system resources.

SC-5 Denial-of-service Protection

Implementation Level 1

Control a. Protect against or limit the effects of the following types of denial-of-service events: events resulting in the prevention of authorised access to a system resource, or delaying system operations and functions; and;

b. Employ the following controls to achieve the denial-of-service objective: Firewalls to protect against Denial of Service attacks.

Considerations Some OT equipment may be more susceptible to DoS attacks due to the time criticality of some OT applications. Risk-based analysis informs the prioritization of DoS protection and the establishment of policy and procedure.

SC-7 Boundary Protection

Implementation Level 1

Control a. Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;

b. Implement subnetworks for publicly accessible system components that are physically and logically separated from internal organizational networks; and

c. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Considerations No additional OT clarification is required for this control.

SC-7(3) Boundary Protection | Access Points

Implementation Level 2

Control Limit the number of external network connections to the system.

Considerations No additional OT clarification is required for this control.

SC-7(4) Boundary Protection | External Telecommunications Services

Implementation Level 2

Control a. Implement a managed interface for each external telecommunication service;

b. Establish a traffic flow policy for each managed interface;

c. Protect the confidentiality and integrity of the information being transmitted across each interface;

d. Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;

e. Review exceptions to the traffic flow policy regularly (e.g. annually) and remove exceptions that are no longer supported by an explicit mission or business need;

f. Prevent unauthorized exchange of control plane traffic with external networks;

g. Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and

h. Filter unauthorized control plane traffic from external networks.

Considerations No additional OT clarification is required for this control.

SC-7(5) Boundary Protection | Deny by Default — Allow by Exception

Implementation Level 2

Control Deny network communications traffic by default and allow network communications traffic by exception at managed interfaces.

Considerations No additional OT clarification is required for this control.

SC-7(7) Boundary Protection | Split Tunneling for Remote Devices

Implementation Level 2

Control Prevent split tunnelling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using safeguards approved by the Architecture Design Authority.

Considerations No additional OT clarification is required for this control.

SC-7(8) Boundary Protection | Route Traffic to Authenticated Proxy Servers

Implementation Level 2

Control Route all traffic (except for approved mutually authenticated communications) to the Internet and Extranets through authenticated proxy servers at managed interfaces.

Considerations No additional OT clarification is required for this control.

SC-7(16) Boundary Protection | Prevent Discovery of System Components

Implementation Level 2

Control Prevent the discovery of specific system components that represent a managed interface.

Considerations	No additional OT clarification is required for this control.

SC-7(18) Boundary Protection | Fail Secure

Implementation Level **3**

Control	Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.
Considerations	The organization selects an appropriate failure mode (e.g., permit or block all communications). The ability to choose the failure mode for the physical part of the OT differentiates the OT from other IT systems. This choice may be a significant influence in mitigating the impact of a failure.

SC-7(21) Boundary Protection | Isolation of System Components

Implementation Level **3**

Control	Employ boundary protection mechanisms to isolate critical system components supporting critical business functions.
Considerations	No additional OT clarification is required for this control.

SC-7(28) Boundary Protection | Connections to Public Networks

Implementation Level **1**

Control	Prohibit the direct connection of IT/OT Systems to a public network.
Considerations	Organizations consider the need for a direct connection to a public network for each OT system, including potential benefits, additional threat vectors, and potential adverse impacts that are specifically relevant to the type of public access that connection introduces. Access to OT should be restricted to the individuals required for operation. A connection made from the OT directly to a public network has limited applicability in OT environments but significant potential risk.

SC-7(29) Boundary Protection | Separate Subnets to Isolate Functions

Implementation Level 2

Control: Implement physically or logically separate subnetworks to isolate the following critical system components and functions: defined critical IT/OT system components and functions.

Considerations: Subnets can be used to isolate low-risk functions from higher-risk ones and control from safety. Subnets should be considered along with other boundary protection technologies.

In OT environments, subnets and zoning are common practices for isolating functions.

SC-8 Transmission Confidentiality and Integrity

Implementation Level 2

Control: Protect the confidentiality and integrity of transmitted information for critical devices and components.

Considerations: No additional OT clarification is required for this control.

SC-8(1) Transmission Confidentiality and Integrity | Cryptographic Protection

Implementation Level 2

Control: Implement cryptographic mechanisms to prevent unauthorized disclosure or detect unauthorized changes to information during transmission.

Considerations: When transmitting across untrusted network segments, the organization explores all possible cryptographic integrity mechanisms (e.g., digital signature, hash function) to protect the confidentiality and integrity of the information. Example compensating controls include physical protections, such as a secure conduit (e.g., point-to-point link) between two system components.

SC-12 Cryptographic Key Establishment and Management

Implementation Level 1

Control: Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: key generation, distribution, storage, access, and destruction in accordance with company policies.

Considerations No additional OT clarification is required for this control.

SC-12(1) Cryptographic Key Establishment and Management | Availability

Implementation Level 3

Control Maintain availability of information in the event of the loss of cryptographic keys by users.

Considerations No additional OT clarification is required for this control.

SC-13 Cryptographic Protection

Implementation Level 1

Control a. Determine the cryptographic uses; and

b. Implement the following types of cryptography required for each specified cryptographic use: Where required by Company or Customer requirements, approved cryptography for each specified cryptographic use.

Considerations No additional OT clarification is required for this control.

SC-15 Collaborative Computing Devices and Applications

Implementation Level 1

Control a. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: Where remote activation has been approved by the appropriate Architecture Design Authority; and

b. Provide an explicit indication of use to users physically present at the devices.

Considerations No additional OT clarification is required for this control.

SC-17 Public Key Infrastructure Certificates

Implementation Level 2

Control a. Issue public key certificates under an approved certificate issuance process or obtain public key certificates from an approved service provider; and

b. Include only approved trust anchors in trust stores or certificate stores managed by the organization.

Considerations No additional OT clarification is required for this control.

SC-18 Mobile Code

Implementation Level 2

Control a. Define acceptable and unacceptable mobile code and mobile code technologies; and

b. Authorize, monitor, and control the use of mobile code within the system.

Considerations No additional OT clarification is required for this control.

SC-20 Secure Name/address Resolution Service (authoritative Source)

Implementation Level 1

Control a. Provide additional data origin authentication and integrity verification artefacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

b. Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.

Considerations Secure name/address resolution services should only be used after careful consideration and verification that they do not adversely impact the operational performance of the OT.

SC-21 Secure Name/address Resolution Service (recursive or Caching Resolver)

Implementation Level 1

Control Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

Considerations Secure name/address resolution services should only be used after careful consideration and verification that they do not adversely impact the operational performance of the OT.

SC-22 Architecture and Provisioning for Name/address Resolution Service

Implementation Level 1

Control: Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation.

Considerations: Secure name/address resolution services should only be used after careful consideration and verification that they do not adversely impact the operational performance of the OT.

SC-23 Session Authenticity

Implementation Level 2

Control: Protect the authenticity of communications sessions.

Considerations: Example compensating controls include auditing measures.

SC-24 Fail in Known State

Implementation Level 3

Control: Fail to a known safe state for the following failures on the indicated components while preserving system state information in failure: for example power failure, process failures, safety interlock activation or override, run time error, component or sensor failure. The Architecture Design Authority is accountable for ensuring that this requirement is included in the system authorisation.

Considerations: The organization selects an appropriate failure state. Preserving OT state information includes consistency among OT state variables and the physical state that the OT represents (e.g., whether valves are open or closed, communication permitted or blocked, continue operations).

As part of the architecture and design of the OT, the organization selects an appropriate failure state in accordance with the function performed by the OT and the operational environment. The ability to choose the failure mode for the physical part of OT differentiates OT systems from other IT systems. This choice may be a significant influence in mitigating the impact of a failure since it may be disruptive to ongoing physical processes (e.g., valves failing in closed position may adversely affect system cooling).

SC-28 Protection of Information at Rest

Implementation Level **2**

Control: Protect the confidentiality and integrity of the following information at rest: All information at rest.

Considerations: Cryptographic mechanisms are implemented only after careful consideration and verification that they do not adversely impact the operational performance of the OT. When cryptographic mechanisms are not feasible on certain OT devices, compensating controls may include relocating the data to a location that does support cryptographic mechanisms.

SC-28(1) Protection of Information at Rest | Cryptographic Protection

Implementation Level **2**

Control: Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on mobile devices such as laptops, smartphones and tablets with full disk encryption on laptops and tablets and container encryption for smartphones. Removable media shall also be encrypted by default.

Considerations: No additional OT clarification is required for this control.

SC-29 Heterogeneity

Implementation Level **2**

Control: Employ a diverse set of information technologies for the following system components in the implementation of the system: Servers, Workstations, Network, Industrial Internet of Things, ICS devices.

Considerations: No additional OT clarification is required for this control.

SC-30 Concealment and Misdirection

Implementation Level **3**

Control: Employ the following concealment and misdirection techniques for critical systems and components during high alert periods, maintenance or critical updates to confuse and mislead adversaries: Honeypots, Honeynets or Decoy systems.

Considerations No additional OT clarification is required for this control.

SC-31 Covert Channel Analysis

Implementation Level 3

Control a. Perform a covert channel analysis to identify those aspects of communications within the system that are potential avenues for covert storage or channels; and

b. Estimate the maximum bandwidth of those channels.

Considerations No additional OT clarification is required for this control.

SC-39 Process Isolation

Implementation Level 1

Control Maintain a separate execution domain for each executing system process.

Considerations Example compensating controls include partition processes to separate platforms.

SC-41 Port and I/O Device Access

Implementation Level 2

Control Physically or Logically disable or remove non-required connection ports or input/output devices on the following systems or system components: IT/OT systems or system components as part of the hardening process.

Considerations No additional OT clarification is required for this control.

SC-44 Detonation Chambers

Implementation Level 3

Control Employ a detonation chamber capability within Security Operation Centre to execute suspicious files in sandboxed environment.

Considerations No additional OT clarification is required for this control.

SC-45 System Time Synchronization

Implementation Level: I

Control: Synchronize system clocks within and between systems and system components.

Considerations: Organizations coordinate time synchronization on OT to allow for accurate troubleshooting and forensics.

Organizations may find relative system time beneficial for many OT systems to ensure the safe and reliable delivery of essential functions. Time synchronization can also make root cause analysis more efficient by ensuring that audit logs from different systems are aligned so that organizations have an accurate view of events across multiple systems when the logs are aggregated.

SC-45(1) System Time Synchronization | Synchronization with Authoritative Time Source

Implementation Level: I

Control: a. Compare the internal system clocks regularly with independent time service; and

b. Synchronize the internal system clocks to the authoritative time source when the time difference is greater than acceptable deviation.

Considerations: Syncing with an authoritative time source may be selected as a control when data is being correlated across organizational boundaries. OT employ suitable mechanisms (e.g., GPS, IEEE 1588) for timestamps.

17 CONTROL FAMILY: SYSTEM AND INFORMATION INTEGRITY

17.1 Control Implementation Levels

Control ID	Control | Control Enhancement	Implementation Level		
SI-1	**Policy and Procedures**	1		
SI-2	**Flaw Remediation**	1		
SI-2(2)	Automated Flaw Remediation Status		2	
SI-3	**Malicious Code Protection**	1		
SI-4	**System Monitoring**	1		
SI-4(2)	Automated Tools and Mechanisms for Real-time Analysis		2	
SI-4(4)	Inbound and Outbound Communications Traffic		2	
SI-4(5)	System-generated Alerts		2	
SI-4(10)	Visibility of Encrypted Communications			3
SI-4(12)	Automated Organization-generated Alerts			3
SI-4(14)	Wireless Intrusion Detection			3
SI-4(20)	Privileged Users			3
SI-4(22)	Unauthorized Network Services			3
SI-5	**Security Alerts, Advisories, and Directives**	1		
SI-5(1)	Automated Alerts and Advisories			3
SI-6	**Security and Privacy Function Verification**			3
SI-7	**Software, Firmware, and Information Integrity**		2	
SI-7(1)	Integrity Checks		2	
SI-7(2)	Automated Notifications of Integrity Violations			3
SI-7(5)	Automated Response to Integrity Violations			3
SI-7(7)	Integration of Detection and Response		2	
SI-7(15)	Code Authentication			3
SI-8	**Spam Protection**		2	
SI-8(2)	Automatic Updates		2	
SI-10	**Information Input Validation**		2	
SI-11	**Error Handling**		2	
SI-12	**Information Management and Retention**	1		
SI-15	**Information Output Filtering**			3
SI-16	**Memory Protection**		2	
SI-17	**Fail-safe Procedures**		2	

17.2 Controls

SI-1 Policy and Procedures

Implementation Level I

Control

a. Develop, document, and disseminate to appropriate personnel or roles:

1. A system and information integrity policy that:
   - a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
   - b. Is consistent with applicable laws, customer requirements, directives, regulations, policies, standards, and guidelines; and
2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;

b. Designate an individual to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and

c. Review and update the current system and information integrity:

1. Policy – e.g. annually and following significant change; and
2. Procedures – e.g. annually and following significant change.

Considerations

The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems.

SI-2 Flaw Remediation

Implementation Level I

Control

a. Identify, report, and correct system flaws;

b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

c. Install security-relevant software and firmware updates within the defined time periods in company Patch Management policy and implementation levels of the release of the updates;

d. Incorporate flaw remediation into the organizational configuration management process.

Considerations

Flaw remediation, or patching, is complicated since many OT employ OSs and other software that are no longer maintained by the vendors. OT operators may also not have the resources or capability to test patches and are dependent on vendors to validate the operability of a patch. Sometimes, the organization has no choice but to accept additional risk if no vendor patch is available, if patching requires additional time to complete validation or testing, or if deployment requires an unacceptable operations shutdown. In these situations, compensating controls should be implemented (e.g., limiting the exposure of the vulnerable system, restricting vulnerable services, implementing virtual patching). Other compensating controls that do not decrease the residual risk but increase the ability to respond may be desirable (e.g., provide a timely response in case of an incident, devise a plan to ensure that the OT can identify exploitation of the flaw). Testing flaw remediation in an OT may exceed the organization's available resources.

SI-2(2) Flaw Remediation | Automated Flaw Remediation Status

Implementation Level 2

Control

Determine if system components have applicable security-relevant software and firmware updates installed using automated mechanisms on a regular basis (e.g monthly).

Considerations

No additional OT clarification is required for this control.

SI-3 Malicious Code Protection

Implementation Level 1

Control

a. Implement signature based or non-signature based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;

c. Configure malicious code protection mechanisms to:

1. Perform periodic scans of the system for networked connected devices (e.g. weekly) and for standalone devices at least in line with the maintenance schedule, if possible under the advice of OEM/system integrator; and real-time scans of files from external sources at endpoint; network entry and exit points as the files are downloaded, opened, or executed in accordance with organizational policy; and

2. Block malicious code; quarantine malicious code; and send alert to the system administrator in response to malicious code detection; and

d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

Considerations

Malicious code protection should only be deployed after careful consideration and verification that it does not adversely impact the operation of the OT. Malicious code protection tools should be configured to minimize their potential impact on the OT (e.g., employ notification rather than quarantine). Example compensating controls include increased traffic monitoring and auditing.

SI-4 System Monitoring

Implementation Level 1

Control

a. Monitor the system to detect:

1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: the identification of external or internal attacks; and

2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through the following techniques and methods: system monitoring, including Insider Threat detection activities;

c. Invoke internal monitoring capabilities or deploy monitoring devices:

1. Strategically within the system to collect organization-determined essential information; and

2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Analyse detected events and anomalies;

e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, or other organizations;

f. Obtain legal opinion regarding system monitoring activities; and

g. Provide correlated, normalized security events to the Security Operations Centre as needed; at the required frequency.

Considerations

The organization ensures that the use of monitoring tools and techniques does not adversely impact the operational performance of the OT. Example compensating controls include deploying sufficient network, process, and physical monitoring.

SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-time Analysis

Implementation Level 2

Control

Employ automated tools and mechanisms to support near real-time analysis of events.

Considerations

When the OT cannot support the use of automated tools for near-real-time analysis of events, the organization employs compensating controls (e.g., providing an auditing capability on a separate system, nonautomated mechanisms or procedures) in accordance with the general tailoring guidance.

SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic

Implementation Level 2

Control

a. Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;

b. Monitor inbound and outbound communications traffic in real time for unusual or unauthorized activities or conditions.

Considerations

No additional OT clarification is required for this control.

SI-4(5) System Monitoring | System-generated Alerts

Implementation Level 2

Control

Alert the local Security Operations Centre and the System Owner when the following system-generated indications of compromise or potential compromise occur: Alarms triggered by correlated, normalized security events.

Considerations

Example compensating controls include manually generating alerts.

SI-4(10) System Monitoring | Visibility of Encrypted Communications

Implementation Level 3

Control

Make provisions so that internal and external encrypted traffic is visible to security network devices/appliance for the purpose of security monitoring.

Considerations

No additional OT clarification is required for this control.

SI-4(12) System Monitoring | Automated Organization-generated Alerts

Implementation Level 3

Control

Alert Security Operation Centre and System Owner using official communication channels and record the incident in ITSM system when the following indications of inappropriate or unusual activities with security or privacy implications occur: insider threat activities, data leakage, system compromise.

Considerations

No additional OT clarification is required for this control.

SI-4(14) System Monitoring | Wireless Intrusion Detection

Implementation Level 3

Control: Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.

Considerations: No additional OT clarification is required for this control.

SI-4(20) System Monitoring | Privileged Users

Implementation Level 3

Control: Implement the following additional monitoring of privileged users: activity logging, behaviour analytics, session recording and period reviews.

Considerations: No additional OT clarification is required for this control.

SI-4(22) System Monitoring | Unauthorized Network Services

Implementation Level 3

Control: a. Detect network services that have not been authorized or approved by Information Security team; and

b. Alert Security Operation Centre and System Owner or System Administrator when detected.

Considerations: No additional OT clarification is required for this control.

SI-5 Security Alerts, Advisories, and Directives

Implementation Level 1

Control: a. Receive system security alerts, advisories, and directives from multiple sources on an ongoing basis;

b. Generate internal security alerts, advisories, and directives as deemed necessary;

c. Disseminate security alerts, advisories, and directives to: Appropriate personnel or roles; interested or impacted elements within the organization; interested or impacted external organizations; and

d. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.

Considerations NCSC-JO generates security alerts and advisories relative to OT.

SI-5(1) Security Alerts, Advisories, and Directives | Automated Alerts and Advisories

Implementation Level 3

Control Broadcast security alert and advisory information throughout the organization using official communication channels, including email notifications and SMS alerts.

Considerations No additional OT clarification is required for this control.

SI-6 Security and Privacy Function Verification

Implementation Level 3

Control a. Verify the correct operation of system integrity;

b. Perform the verification of the functions specified in SI-6a: system startup, restart, shutdown, and abort; upon command by user with appropriate privilege; at least annually;

c. Alert System Owner or System Administrator to failed security and privacy verification tests; and

d. Isolate the system when anomalies are discovered.

Considerations No additional OT clarification is required for this control.

SI-7 Software, Firmware, and Information Integrity

Implementation Level 2

Control a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: Software, firmware, and information deemed inscope given its criticality; and

b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: Inform Service Provider, Business Owner and raise a security incident in ITSM or Risk Management system.

Considerations The organization determines whether the use of integrity verification applications would adversely impact operation of the ICS and employs compensating controls (e.g., manual integrity verifications that do not affect performance).

SI-7(1) Software, Firmware, and Information Integrity | Integrity Checks

Implementation Level **2**

Control Perform an integrity check of software, firmware, and information: at startup; at transitional states or security-relevant events; regularly (e.g. daily).

Considerations The organization ensures that the use of integrity verification applications does not adversely impact the operational performance of the OT.

SI-7(2) Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations

Implementation Level **3**

Control Employ automated tools that provide notification to System Owner and System Administrator upon discovering discrepancies during integrity verification.

Considerations When the organization cannot employ automated tools that provide notifications about integrity discrepancies, the organization employs nonautomated mechanisms or procedures. Example compensating controls include performing scheduled manual inspections for integrity violations.

SI-7(5) Software, Firmware, and Information Integrity | Automated Response to Integrity Violations

Implementation Level **3**

Control Automatically shut the system down and implement isolation controls when integrity violations are discovered and alert Security Operation Centre Team and System Owner.

Considerations Shutting down and restarting the ICS may not always be feasible upon identification of an anomaly. These actions should be scheduled according to ICS operational requirements.

SI-7(7) Software, Firmware, and Information Integrity | Integration of Detection and Response

Implementation Level 2

Control: Incorporate the detection of the following unauthorized changes into the organizational incident response capability: Changes not approved by the relevant change management process.

Considerations: When the ICS cannot detect unauthorized security- relevant changes, the organization employs compensating controls (e.g., manual procedures) in accordance with the general tailoring guidance.

SI-7(15) Software, Firmware, and Information Integrity | Code Authentication

Implementation Level 3

Control: Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: System updates or firmware updates.

Considerations: Code authentication provides assurance that the software and firmware have not been tampered with. If automated mechanisms are not available, organizations could manually verify code authentication by using a combination of techniques, including verifying hashes, downloading from reputable sources, verifying version numbers with the vendor, or testing software and firmware in offline or test environments.

SI-8 Spam Protection

Implementation Level 2

Control: a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and

b. Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.

Considerations: OT organizations implement spam protection by removing spam transport mechanisms, functions, and services (e.g., electronic mail, web browsing) from the OT.

SI-8(2) Spam Protection | Automatic Updates

Implementation Level 2

Control: Automatically update spam protection mechanisms regularly (e.g. on a weekly basis).

Considerations No additional OT clarification is required for this control.

SI-10 Information Input Validation

Implementation Level **2**

Control Check the validity of the following information inputs: All information inputs to the system.

Considerations No additional OT clarification is required for this control.

SI-11 Error Handling

Implementation Level **2**

Control a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and

b. Reveal error messages only to systems administrators, application administrators or service providers.

Considerations No additional OT clarification is required for this control.

SI-12 Information Management and Retention

Implementation Level **1**

Control Manage and retain information within the system and information output from the system in accordance with applicable laws, customer requirements, directives, regulations, policies, standards, guidelines and operational requirements.

Considerations No additional OT clarification is required for this control.

SI-15 Information Output Filtering

Implementation Level **3**

Control Validate information output from the following software programs and/or applications to ensure that the information is consistent with the expected content: Critical applications, Industrial Internet of Things, SCADA, ICS, and PLC devices.

Considerations No additional OT clarification is required for this control.

SI-16 Memory Protection

Implementation Level 2

Control Implement the following controls to protect the system memory from unauthorized code execution: Data execution prevention or address space layout randomization.

Considerations No additional OT clarification is required for this control.

SI-17 Fail-safe Procedures

Implementation Level 2

Control Implement the indicated fail-safe procedures when the indicated failures occur:
Each IT/OT environment owner shall define a list of failure conditions and associated fail-safe procedures that must be followed from a Safety and/or Security perspective.

Considerations The selected failure conditions and corresponding procedures may vary among baselines. The same failure event may trigger different responses, depending on the impact level. Mechanical and analog systems can be used to provide mechanisms to ensure fail-safe procedures. Fail-safe states should incorporate potential impacts to human safety, physical systems, and the environment. A related controls is CP-6.

18 CONTROL FAMILY: SUPPLY CHAIN RISK MANAGEMENT

18.1 Control Implementation Levels

Control ID	**Control |** Control Enhancement	Implementation Level		
SR-1	**Policy and Procedures**	1		
SR-2	**Supply Chain Risk Management Plan**	1		
SR-2(1)	Establish SCRM Team			3
SR-3	**Supply Chain Controls and Processes**	1		
SR-3(1)	Diverse Supply Base		2	
SR-4	**Provenance**			3
SR-5	**Acquisition Strategies, Tools, and Methods**	1		
SR-5(1)	Adequate Supply		2	
SR-6	**Supplier Assessments and Reviews**		2	
SR-8	**Notification Agreements**	1		
SR-9	**Tamper Resistance and Detection**			3
SR-9(1)	Multiple Stages of System Development Life Cycle			3
SR-10	**Inspection of Systems or Components**	1		
SR-11	**Component Authenticity**	1		
SR-11(1)	Anti-counterfeit Training		2	
SR-11(2)	Configuration Control for Component Service and Repair		2	
SR-12	**Component Disposal**	1		

18.2 Controls

SR-1 Policy and Procedures

Implementation Level 1

Control a. Develop, document, and disseminate to appropriate personnel or roles:

1. An Organization-level; Mission/business process-level; System-level supply chain risk management policy that:

a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;

b. Designate an individual to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and

c. Review and update the current supply chain risk management:

1. Policy - e.g. annually and following significant change; and
2. Procedures - e.g. annually and following significant change.

Considerations Supply chain policies and procedures for OT should consider both components received and components produced. Many OT systems use legacy components that cannot meet modern supply chain expectations. Appropriate compensating controls should be developed to achieve organizational supply chain expectations for legacy systems.

SR-2 Supply Chain Risk Management Plan

Implementation Level 1

Control a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: systems, system components, or system services;

b. Review and update the supply chain risk management plan regularly (e.g. annually) or as required, to address threat, organizational or environmental changes; and

c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

Considerations No additional OT clarification is required for this control.

SR-2(1) Supply Chain Risk Management Plan | Establish SCRM Team

Implementation Level 3

Control Establish a supply chain risk management team consisting of appropriate personnel to perform Supply Chain Rism Management (SCRM) activity to lead and support the following SCRM activities: The identification, treatment and mitigation of SCRM concerns.

Considerations No additional OT clarification is required for this control.

SR-3 Supply Chain Controls and Processes

Implementation Level: 1

Control

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of system or system components or system services for those items identified within the plan created in SR-2, in coordination with the personnel identified in the Supply Chain Risk Management Plan (SR-2);

b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: Supplier onboarding activities; ongoing supplier management processes; and

c. Document the selected and implemented supply chain processes and controls in appropriate documentation to be defined by the Organization.

Considerations

No additional OT clarification is required for this control.

SR-3(1) Supply Chain Controls and Processes | Diverse Supply Base

Implementation Level: 2

Control

Employ a diverse set of sources for the following system components and services:

a. Suppliers

b. Partners

c. Contractors

Considerations

Using a diverse set of suppliers in the OT environment can improve reliability by reducing common cause failures. This is not always possible since some technologies have limited supply options that meet the operational requirements.

SR-4 Provenance

Implementation Level: 3

Control

Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: critical systems and components, critical storage and data.

Considerations

No additional OT clarification is required for this control.

SR-5 Acquisition Strategies, Tools, and Methods

Implementation Level: 1

Control: Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: Appropriate acquisition strategies, contract tools, and procurement methods, as defined in the output from SR-2.

Considerations: No additional OT clarification is required for this control.

SR-5(1) Acquisition Strategies, Tools, and Methods | Adequate Supply

Implementation Level: 2

Control: Employ the following controls to ensure an adequate supply of critical components is available to meet operational needs; ensure this is coordinated with what is defined in SR-2 and the Contingency Plan (CP-2).

Considerations: Vendor relationships and spare parts strategies are developed to ensure that an adequate supply of critical components is available to meet operational needs.

OT systems and system components are often built for purpose and have a limited number of vendors or suppliers for a specific component. Organizations identify critical OT system components and controls to ensure an adequate supply in the event of supply chain disruptions.

SR-6 Supplier Assessments and Reviews

Implementation Level: 2

Control: Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide regularly (e.g. on a least an annual basis), as detailed in the output from SR-2 and in line with the agreed review cycle of this document.

Considerations: No additional OT clarification is required for this control.

SR-8 Notification Agreements

Implementation Level: 1

Control: Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the notification of supply chain compromises and results of assessments or audits.

Considerations No additional OT clarification is required for this control.

SR-9 Tamper Resistance and Detection

Implementation Level 3

Control Implement a tamper protection program for the system, system component, or system service.

Considerations No additional OT clarification is required for this control.

SR-9(1) Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle

Implementation Level 3

Control Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.

Considerations No additional OT clarification is required for this control.

SR-10 Inspection of Systems or Components

Implementation Level 1

Control Inspect the following systems or system components randomly; when returning from a high-risk location, or upon suspicion to detect tampering: hardware, firmware and software systems or system components.

Considerations No additional OT clarification is required for this control.

SR-11 Component Authenticity

Implementation Level 1

Control a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and

b. Report counterfeit system components to source of counterfeit component, and raise a Security incident in ITSM or Risk Management system.

Considerations No additional OT clarification is required for this control.

SR-11(1) Component Authenticity | Anti-counterfeit Training

Implementation Level 2

Control Train appropriate personnel or roles to detect counterfeit system components (including hardware, software, and firmware).

Considerations No additional OT clarification is required for this control.

SR-11(2) Component Authenticity | Configuration Control for Component Service and Repair

Implementation Level 2

Control Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: For defined critical system components.

Considerations No additional OT clarification is required for this control.

SR-12 Component Disposal

Implementation Level 1

Control Dispose of data, documentation, tools, or system components using the following techniques and methods: Approved techniques and methods compliant with any Legal, Regulatory, Customer or Company requirements.

Considerations No additional OT clarification is required for this control.

19 GLOSSARY

Common terms used in this document:

Activities	An assessment object that includes specific protection-related pursuits or actions supporting an information system that involve people (e.g., conducting system backup operations, monitoring network traffic).
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticator	The means used to confirm the identity of a user, process, or device (e.g. user password or token).
Authorizing Official (AO)	The individual with the responsibility to authorise the operation and acceptable level of risk of an information system. Depending upon context, this may be a Business Owner of a System – e.g. to authorize access to a system – or a Security Authority. Authorizing officials typically have budgetary oversight for the system or are responsible for the mission and/or business operations supported by the system. Accordingly, authorizing officials are in management positions with a level of authority commensurate with understanding and accepting such security and privacy risks.
Authorizing Official Designated Representative	The authorizing official designated representative is an organizational official designated by the authorizing official (AO) who is empowered to act on behalf of the authorizing official to coordinate and conduct the day-to-day activities associated with managing risk to information systems and organizations. The only activity that cannot be delegated by the authorizing official to the designated representative is the authorization decision and signing of the associated authorization decision document (i.e. the acceptance of risk).
Business Critical Systems	Applications and data deemed critical to the ongoing successful functioning of the business. For such systems and data, these will typically be covered by an organisation's IT/OT and service continuity plans as appropriate.
Change	ITIL (Information Technology Infrastructure Library) distinguishes between three different types of Changes: 1. Standard Changes: Pre-authorized, low-risk Changes that follow a well-known procedure. 2. Emergency Changes: Changes that must be implemented immediately, for example to resolve a Major Incident. 3. Normal Changes: All other Changes that are not Standard Changes or Emergency Changes.

	Normal Changes can be further categorized as Major, Significant or Minor, depending on the level of risk involved and might be expected to have designated individuals or structures responsible for approving them, depending on their significance.
Computing Device	Any fixed, portable, or mobile computer system capable of transmitting, processing or storing information. This includes network equipment, smart phones, cameras, and multimedia devices.
Cyber Security	For the purposes of this standard, this is the measures taken to protect information systems and networks and critical infrastructures from cyber security incidents and the ability to return them to their running order and continuation; not withstanding whether those were accessed without authorisation, by misuse or as a result of failing to follow security measurers or being subject to deception leading thereto.
Enterprise Network/System	A Network/System operated across multiple business units by Enterprise IT Services.
Extranet	Externally accessible network that contains partner, customer and supplier systems.
Hard Token	A token that is based on a unique physical device that is used to display or generate the user's onetime passcode on use.
Human Machine Interfaces (HMIs)	The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a colour graphics display running dedicated HMI software. Operators and engineers use HMIs to monitor and configure set points, control algorithms, and adjust and establish parameters in the controller. The HMI also displays process status information and historical information.
Incident	An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
Industrial Control System (ICS)	General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC) found in the industrial sectors and critical infrastructures. An industrial control system consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy).

Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Owner	A senior member of a business unit or function with business ownership of an Information System.
ITSM	IT Service Management
JNCSF	Jordan National Cyber Security Framework
LAN	Local Area Network (contained within a site or single location).
Malware	Any program or file that is designed to damage or do other unwanted actions on a computer system, user or data (e.g., computer viruses, worms, Trojan horses, adware, and also spyware - programming that gathers information about a computer user without permission).
Mobile Code	Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient. Examples include Java applets, JavaScript, HTML5, WebGL, and VBScript.
Mobile Device	A mobile device is a computing device that has a small form factor such that it can be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable or removable data storage; and includes a self-contained power source. Examples include laptops, tablets and mobile 'phones.
Multifactor Authentication	Authentication using two or more different factors to achieve authentication. Factors include (i) something you know (password/PIN) (ii) something you have (cryptographic identification device, token) and (iii) something you are (biometric).
Network	The wired and wireless infrastructure that interconnects an organisation's systems computing assets including Voice over Internet Protocol (VoIP).
NIST SP 800-53	National Institute of Standards and Technology Special Publication – Security and Privacy Controls for Federal Information Systems and Organizations.
NIST SP 800-82	National Institute of Standards and Technology Special Publication – Guide to Operational Technology (OT) Security.
Non-Interactive	Not interacting with the screen/keyboard (i.e. Non-Interactive User).

Operational Technology (OT)	A broad range of programmable systems and devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems and devices detect or cause a direct change through monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.
OEM	Original Equipment Manufacturer
PKI	Public Key infrastructure is a set of roles, policies, and procedures to create, manage, distribute, use, store and revoke digital certificates.
Privileged Users / Accounts	Users or Accounts that have been granted additional special capabilities over and above a standard User account. This may include local administrator capability, the ability to write to removable media, or may include elevated applications access, such as the ability to authorise payment transactions.
Highly Privileged Users / Accounts	Users or Accounts that have been granted privileges that are wide-ranging in their capabilities, often at a server of infrastructure level – e.g. "Administrator" / "Root" / "Super User" / "Domain Admin".
Portable Storage Device	A system component that can communicate with and be added to or removed from a system or network and that is limited to data storage—including text, video, audio or image data—as its primary function (e.g., optical discs, external or removable hard drives, external or removable solid-state disk drives, magnetic or optical tapes, flash memory devices, flash memory cards, and other external or removable disks).
Registration Authority	A trusted entity that establishes and vouches for the identity and authorization of a certificate applicant on behalf of some authority.
Regulatory Authority	For cyber security this refers to the NCSC-JO.
Remote Access	Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network.
Security Authority	The senior leadership person appointed by the Line Leader to ensure that security within the Business is compliant and effective.
Sensitive Information	Information that requires additional protection and may also require special marking or handling. This could include company information, customer information, and personal information, and other controlled information deemed sensitive by the organisation.

Security Information and Event Management Tool (SIEM)	An application that provides the ability to gather security data from information system components and present that data as actionable information via a single interface.
Service Account	A special computer account that may be granted special rights, administrative or otherwise, to run software or processes, typically in a non-interactive process.
Shared Account	A single account that can be accessed by multiple individuals through the use of a shared password.
Strength of Mechanism (SoM)	A scale for measuring the relative strength of a security mechanism (a device, method or function designed to achieve a security purpose).
System	Combination of interacting elements organized to achieve one or more stated purposes. See also "Information System" in this Glossary.
Users	Any Employee, contractor, IT service provider, consultant, temporary staff, and any other individual employing or accessing Company IT Assets, including all personnel affiliated with third parties.
VLAN	Virtual Local Area Network – A VLAN is a configuration that creates logical networks that are partitioned and isolated within a network.
VPN	Virtual Private Network – A VPN is a method for accessing a remote network via secure "tunnelling" through another network such as the Internet.
WAN	Wide Area Network (Network connecting multiple sites or locations).

For any other terms, please see NIST Special Publication 800-53 Revision 5: a full glossary is incorporated in the document at Appendix A; a list of Acronyms is included at Appendix B. A wider NIST glossary is also available via the NIST Computer Security Resource Center.

المركـز الوطني للأمـن السيبرانـي
National Cyber Security Center