AFROSAI-E

Cyber Security Technical Guide

EXPOSURE DRAFT

DECEMBER 2023

Issued in South Africa

First Edition (Exposure Draft), December 2023

Table of Contents

OVERVIEW 2

AC – ACCESS CONTROL 6

AT – AWARENESS AND TRAINING 21

AU – ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT 25

SAA – SECURITY ASSESSMENT AND AUTHORISATION 35

CM – CONFIGURATION MANAGEMENT 44

CP – CONTINGENCY PLANNING 53

IA – IDENTIFICATION AND AUTHENTICATION 63

IR – INCIDENT RESPONSE 73

MA – MAINTENANCE 80

PE – PHYSICAL AND ENVIRONMENTAL PROTECTION 88

PL – PLANNING 99

PM – PROGRAMME MANAGEMENT 103

PS – PERSONNEL SECURITY 115

RA – RISK ASSESSMENT 123

SA – SYSTEM AND SERVICE ACQUISITION 130

SA-5 | SYSTEM DOCUMENTATION 134

SC – SYSTEM AND COMMUNICATION PROTECTION 140

SI – SYSTEM AND INFORMATION INTEGRITY 151

SR – SUPPLY CHAIN RISK MANAGEMENT 159

1. OVERVIEW

PURPOSE

The purpose of the Cybersecurity technical guide is to provide the AFROSAI-E member institutions with specific guidance for implementing security controls in a format that easily aligns with global standards, including ISO 27001:2022, COBIT, CIS Controls but specifically the National Institute of Standards and Technology Special Publication 800-53 Revision 5 (NIST 800-53 Revision 5).

APPLICATION OF MORE STRINGENT STANDARDS

This document specifies the minimum baselines for information security controls for all *member institutions* and their information resources. Controls in this document are not exclusively technical; therefore, their application is not inherently limited to information systems.

Each AFROSAI-E *member institution* may select and apply any additional security controls, control baselines, or control enhancements for information resources or scenarios where an elevated security posture is required to mitigate risks identified by the member institutions.

For systems that store, process, or transmit confidential and/or information subject to other security regulatory requirements, additional security controls or control baselines shall be selected and applied commensurate with the level of risk and confidentiality, integrity, and availability requirements of the system.

DOCUMENT LIFECYCLE

Before publishing new or revised standards, AFROSAI-E will solicit comments on new controls from ICT Managers, Risk Managers, Information Security Managers and other relevant stakeholders from all the member institutions.

REVISION HISTORY

Version	Date	Change Description
Draft Version 1.0	August 2022	Creation of Draft Document

NUMBER OF CONTROLS BY FAMILY

ID	Control Family	Number of Controls/Enhancements
AC	Access Control	13
AT	Awareness and Training	4
AU	Accountability, Audit, and Risk Management	10
SAA	Security Assessment and Authorisation	9
CM	Configuration Management	9
CP	Contingency Planning	8
IA	Identification and Authentication	10
IR	Incident Response	9
MA	Maintenance	4
MP	Media Protection	4
PE	Physical and Environmental Protection	11
PL	Planning	3
PM	Programme Management	12
PS	Personnel Security	8
RA	Risk Assessment	6
SA	System and Service Acquisition	10
SC	System and Communication Protection	11
SI	System and Information Integrity	7
SR	Supply Chain Risk Management	6
	Total	**154**

CONTROL DETAILS AND SAMPLE FORMAT

Each control group is organised under its group identification code and title, *e.g.,* **AC – ACCESS CONTROL.**

Information about each control is presented in the following format.

[Control ID] [Control Name]

CONTROL DESCRIPTION: This field provides information on how the control can be implemented.

IMPLEMENTATION DETAILS: This field provides specific guidance or additional requirements that apply to the control and must be incorporated into the implementation of the control.

2. AC – ACCESS CONTROL

AC-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to *organisation-defined* personnel or roles:

    i. An access control policy that:
        a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among institutional personnel, and compliance; and
        b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
    ii. Procedures to facilitate the implementation of the access control policy and the associated access controls.
2. Designate an *organisation-defined* official to manage the development, documentation, and dissemination of the access control policy and procedures; and
3. Review and update the current access control:
    i. Policy as per *organisation-defined frequency*; and
    ii. Procedures as per *organisation-defined frequency*.

IMPLEMENTATION DETAILS

Reference the control description above.

AC-2 | ACCOUNT MANAGEMENT

CONTROL DESCRIPTION

1. Define and document the types of accounts allowed for use within the system.
2. Assign account managers.
3. Establish conditions for group and role membership.
4. Specify:
    - Authorised users of the system.
    - Group and role membership; and
    - Access authorisations (i.e., privileges).

5. Require approvals by defined personnel or roles for requests to create accounts.
6. Create, enable, modify, disable, and remove accounts by [*organisation*-defined] policy, procedures, and conditions
7. Monitor the use of accounts.
8. Notify account managers and [*organisation-defined* personnel or roles] within:
    - [organisation-defined time-period] when accounts are no longer required.
    - [organisation-defined time-period] when users are terminated or transferred; and
    - [organisation-defined time-period] when system usage or need-to-know changes for an individual.

9. Authorise access to the system based on:
    - A valid access authorisation.
    - Intended system usage; and
    - Additional [organisation-defined attributes (as required)].

10. Review accounts for compliance with account management requirements [organisation-defined frequency].
11. Establish and implement a process for changing shared or group account credentials (if deployed) when individuals are removed from the group; and
12. Align account management processes with personnel termination and transfer processes.

IMPLEMENTATION DETAILS

Confidential information shall be accessible only to authorised users. An information file or record containing confidential information shall be identified, documented, and protected. Information resources assigned from or shared between one Supreme Audit Institution (SAI) to another or from or between an SAI to a contractor or other third party shall be protected by the conditions imposed by the providing SAI at a minimum.

AC-3 | ACCESS ENFORCEMENT

CONTROL DESCRIPTION

Enforce approved authorisations for logical access to information and system resources by applicable access control policies.

IMPLEMENTATION DETAILS

1. Access to information resources shall be appropriately managed.

2. Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resources system may grant that user access.

AC-5 | SEPARATION OF DUTIES

CONTROL DESCRIPTION

1. Identify and document [*organisation-defined* duties of individuals requiring separation]; and
2. Define system access authorisations to support separation of duties.

IMPLEMENTATION DETAILS

Reference the control description above.

AC-6 | LEAST PRIVILEGE

CONTROL DESCRIPTION

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

IMPLEMENTATION DETAILS

Reference the control description above.

AC-7 | UNSUCCESSFUL LOGON ATTEMPTS

CONTROL DESCRIPTION

1. Enforce a limit of [*organisation-defined number*] consecutive invalid logon attempts by a user during a [*organisation-defined time-perio*d]; and

2. Automatically [Select (one or more)]: lock the account for an [organisation-defined time-period]; lock the account until released by an administrator; delay next logon prompt per [organisation-defined delay algorithm]; notify system administrator; take other [organisation-defined action] when the maximum number of unsuccessful attempts is exceeded.

IMPLEMENTATION DETAILS

1. As technology permits, (AFROSAI-E [member institution] shall enforce account lockouts after, at minimum, ten failed attempts. This threshold may be lowered for Moderate or High-risk systems.

2. Accounts locked out due to multiple incorrect logon attempts shall stay locked out for a minimum of 15 minutes. Accounts for Moderate or High-risk systems shall remain locked until reset by an administrator.

AC-8 | SYSTEM USE NOTIFICATION

CONTROL DESCRIPTION

1. Display [organisation-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and that:

    i. Users are accessing an organisation system;
    ii. System usage may be monitored, recorded, and subject to audit;
    iii. Unauthorised use of the system is prohibited and subject to criminal and civil penalties; and
    iv. Use of the system indicates consent to monitoring and recording.

2. 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
3. For publicly accessible systems:

    i. Display system use information [organisation-defined conditions] before granting further access to the publicly accessible system;
    ii. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
4. Include a description of the authorised uses of the system.

IMPLEMENTATION DETAILS

System Identification/Logon Banner. System identification/logon banners shall have warning statements that include the following topics:

- Unauthorised use is prohibited;
- Usage may be subject to security testing and monitoring;
- Misuse is subject to criminal prosecution; and
- Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

AC-14 | PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

CONTROL DESCRIPTION

1. Identify [organisation-defined user actions] that can be performed on the system without identification or authentication consistent with organisational missions and business functions; and

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

IMPLEMENTATION DETAILS

Reference the control description above.

AC-17 | REMOTE ACCESS

CONTROL DESCRIPTION

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

b. Authorise each type of remote access to the system before allowing such connections.

IMPLEMENTATION DETAILS

Reference the control description above.

AC-18 | WIRELESS ACCESS

CONTROL DESCRIPTION

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

2. Authorise each type of wireless access to the system before allowing such connections.

IMPLEMENTATION DETAILS

SAIs shall establish the requirements and security restrictions for installing or providing access to the SAI's information resources systems. The wireless policy shall address the following topic areas:

i. Wireless Local Area Networks. Ensure that Service Set Identifiers (SSID) values are changed from the manufacturer's default setting. Some networks should not include organisational or location information in the SSID.

ii. Transmitting and Encrypting Information. Types of information that may be transmitted via wireless networks and devices, with or without encryption, including mission-critical information or sensitive personal information.

iii. SAIs shall not transmit confidential information via a wireless connection to or from a portable computing device unless encryption methods, such as a Virtual Private Network (VPN), Wi-Fi Protected Access, or other secure encryption protocols that meet appropriate protection or certification standards as detailed within this Security Control Standards Document, are used to protect the information.

iv. Installation or use of Wireless Personal Area Networks. Prohibit and periodically monitor any unauthorised installation or use of Wireless Personal Area Networks on SAI IT systems by individuals without the approval of the institution's information resources manager.

AC-19 | ACCESS CONTROL FOR MOBILE DEVICES

CONTROL DESCRIPTION

1. Establish configuration requirements, connection requirements, and implementation guidance for organisation-controlled mobile devices, including when such devices are outside of controlled areas; and

2. Authorise the connection of mobile devices to organisational systems.

IMPLEMENTATION DETAILS

Reference the control description above.

AC-20 | USE OF EXTERNAL SYSTEMS

CONTROL DESCRIPTION

Establish terms and conditions or controls asserted to be implemented on external systems consistent with the trust relationships established with other organisations owning, operating, and/or maintaining external systems, allowing authorised individuals to:

i. Access the system from external systems; and
ii. Process, store, or transmit organisation-controlled information using external systems.

IMPLEMENTATION DETAILS

Reference the control description above.

AC-21 | PUBLICLY ACCESSIBLE CONTENT

CONTROL DESCRIPTION

1. Define and document the information types intended to be publicly available. Categorise this information based on its sensitivity, nature, and intended audience.
2. Specify the procedures and conditions for publishing information to public platforms or websites.
3. Establish a process for reviewing and approving what information is suitable for public release. This should involve relevant personnel or roles to ensure that sensitive or confidential data is not inadvertently disclosed.
4. Designate individuals authorised to make information publicly accessible.
5. Train authorised individuals to ensure publicly accessible information does not contain non-public information.
6. Review the proposed content of information before posting it onto the publicly accessible system to ensure that non-public information is not included; and
7. Review the content on the publicly accessible system for non-public information [organisation-defined frequency] and remove such information if discovered.

IMPLEMENTATION DETAILS

Reference the control description above.

AC-22 | PASSWORD MANAGEMENT

CONTROL DESCRIPTION

1. Document a comprehensive password policy defining the rules for creating and managing passwords. Include requirements for password length, complexity, expiration, and history.

IMPLEMENTATION DETAILS

1. Enforce password complexity rules, requiring a combination of uppercase letters, lowercase letters, numbers, and special characters.
2. Implement password expiration policies that force users to change their passwords regularly.
3. Keep a history of previous passwords to prevent users from reusing them too quickly.
4. Implement account lockout mechanisms that temporarily lock an account after a specified number of unsuccessful login attempts.
5. Consider implementing 2FA to add an extra layer of security to user accounts.
6. Consider storing passwords securely by using strong cryptographic hashing algorithms.
7. Consider developing a secure process for password recovery and reset that verifies the identity of the user requesting the change.
8. Maintain detailed logs of password-related events and regularly review them for any security incidents.

AT – AWARENESS AND TRAINING

AT-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to defined member institution personnel or roles:

    i. An awareness and training policy that:
        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and
        - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

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

2. Designate an [organisation-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and

3. Review and update the current awareness and training:

    i. Policy [organisation-defined frequency]; and
    ii. Procedures [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

AT-2 | AWARENESS TRAINING

CONTROL DESCRIPTION

1. Provide security and privacy awareness training to system users (including managers, senior executives, and contractors):

    i. As part of initial training for new users and [organisation-defined frequency] thereafter; and
    ii. When required by system changes; and

2. Update awareness training [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

AT-3 | ROLE-BASED TRAINING

CONTROL DESCRIPTION

1. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [organisation-defined roles and responsibilities]:

    i. Before authorising access to the system, information, or performing assigned duties, and [organisation-defined frequency] thereafter; and
    ii. When required by system changes; and

2. Update role-based training [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

AT-4 | TRAINING RECORDS

CONTROL DESCRIPTION

1. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and

2. Retain individual training records for [organisation-defined period].

IMPLEMENTATION DETAILS

Reference the control description above.

AU – ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT

AU-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to [organisation-defined personnel or roles]:

    i. [Select (one or more)]: [organisation-level; mission/business process-level; system- level] audit and accountability policy that:

        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and
        - Is consistent with applicable laws, executive orders, 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;

3. Designate an [organisation-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and

4. Review and update the current audit and accountability:

    i. Policy [organisation-defined frequency]; and
    ii. Procedures [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

AU-2 | EVENT LOGGING

CONTROL DESCRIPTION

1. Identify the types of events that the system can log in support of the audit function: organisation-defined event types that the system can log.

2. Coordinate the event logging function with other organisational entities requiring audit-related information to guide and inform the selected criteria for event logging.

3. Specify the following event types for logging within the system: [organisation-defined event types (a subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type].

4. 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

5. Review and update the event types selected for logging [organisation-defined frequency].

IMPLEMENTATION DETAILS

Information resources systems shall provide the means whereby authorised personnel can audit and establish individual accountability for any action that can potentially cause access to, generation or modification of, or affect the release of confidential information.

Appropriate audit trails shall be maintained to provide accountability for updates to mission-critical information, hardware and software and all changes to automated security or access rules.

Based upon an SAI's assessment of the risk, the SAI shall maintain a sufficiently complete history of transactions to permit an audit of the information resources system by logging and tracing the activities of individuals through the system.

AU-3 | CONTENT OF AUDIT RECORDS

CONTROL DESCRIPTION

1. Ensure that audit records contain information that establishes the following:

    i. What type of event occurred?
    ii. When the event occurred; c. Where the event occurred; d. Source of the event;
    iii. The outcome of the event; and
    iv. Identity of any individuals, subjects, or objects/entities associated with the event.

IMPLEMENTATION DETAILS

Reference the control description above.

AU-4 | AUDIT LOG STORAGE CAPACITY

CONTROL DESCRIPTION

Allocate audit log storage capacity to accommodate [organisation-defined audit log retention requirements].

IMPLEMENTATION DETAILS

Reference the control description above.

AU-5 | RESPONSE TO AUDIT LOGGING PROCESS FAILURES

CONTROL DESCRIPTION

1. Alert [organisation-defined personnel or roles] within [organisation- defined time-period] in the event of an audit logging process failure; and

2. Take the following additional actions: [organisation-defined additional actions].

IMPLEMENTATION DETAILS

Reference the control description above.

AU-6 | AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

CONTROL DESCRIPTION

1. Review and analyse system audit records [organisation-defined frequency] for indications of [organisation-defined inappropriate or unusual activity].

2. Report findings to [organisation-defined personnel or roles]; and

3. 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.

IMPLEMENTATION DETAILS

Reference the control description above.

AU-8 | TIME STAMPS

CONTROL DESCRIPTION

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

2. Record time stamps for audit records that meet [organisation-defined granularity of time measurement] and use Coordinated Universal Time to have a fixed local time offset from Coordinated Universal Time or include the local time offset as part of the time stamp.

IMPLEMENTATION DETAILS

Reference the control description above.

AU-9 | PROTECTION OF AUDIT INFORMATION

CONTROL DESCRIPTION

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

IMPLEMENTATION DETAILS

Reference the control description above.

AU-11 | AUDIT RECORD RETENTION

CONTROL DESCRIPTION

Retain audit records for [organisation-defined time-period consistent with records retention policy] to support after-the-fact investigations of incidents and meet regulatory and organisational information retention requirements.

IMPLEMENTATION DETAILS

Reference the control description above.

AU-12 | AUDIT RECORD GENERATION

CONTROL DESCRIPTION

1. Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [organisation-defined system components];

2. Allow [organisation-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and

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

IMPLEMENTATION DETAILS

Reference the control description above.

SAA – SECURITY ASSESSMENT AND AUTHORISATION

SAA-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to [organisation-defined personnel or roles]:

    i. [Select (one or more): organisation-level; mission/business process-level; system- level] assessment, authorisation, and monitoring policy that:

        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and
        - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

    ii. Procedures to facilitate the implementation of the assessment, authorisation, and monitoring policy and the associated assessment, authorisation, and monitoring controls;

2. Designate an [organisation-defined official] to manage the development, documentation, and dissemination of the assessment, authorisation, and monitoring policy and procedures; and

3. Review and update the current assessment, authorisation, and monitoring:

    i. Policy [organisation-defined frequency]; and
    ii. Procedures [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

SAA-2 | CONTROL ASSESSMENTS

CONTROL DESCRIPTION

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

    i. Controls and control enhancements under assessment;
    ii. Assessment procedures to be used to determine control effectiveness; and
    iii. Assessment environment, assessment team, and assessment roles and responsibilities;

2. Ensure the control assessment plan is reviewed and approved by the authorising official or designated representative before conducting the assessment;

3. Assess the controls in the system and its environment of operation [organisation-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome concerning meeting established security and privacy requirements;

4. Produce a control assessment report that documents the results of the assessment; and

5. Provide the results of the control assessment to [organisation-defined individuals or roles].

IMPLEMENTATION DETAILS

A review of the SAI's information security programme for compliance with these standards will be performed biennially based on business risk management decisions by an individual(s) independent of the information security programme and designated by the SAI head or their designated representative(s).

SAA-3 | INFORMATION EXCHANGE

CONTROL DESCRIPTION

1. Approve and manage the exchange of information between the system and other systems using [Select (one or more)]: interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; [organisation-defined type of agreement];

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

3. Review and update the agreements [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

SAA-5 | PLAN OF ACTION AND MILESTONES

CONTROL DESCRIPTION

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

2. Update the existing plan of action and milestones [organisation-defined frequency] based on the findings from control assessments, audits, and continuous monitoring activities.

IMPLEMENTATION DETAILS

Reference the control description above.

SAA-6 | AUTHORISATION

CONTROL DESCRIPTION

1. Assign a senior official as the authorising official for the system;

2. Assign a senior official as the authorising official for common controls available for inheritance by organisational systems;

3. Ensure that the authorising official for the system, before commencing operations:

    i. Accepts the use of common controls inherited by the system; and
    ii. Authorises the system to operate;

4. Ensure that the authorising official for common controls authorises the use of those controls for inheritance by organisational systems;

5. Update the authorisations [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

SAA-7 | CONTINUOUS MONITORING

CONTROL DESCRIPTION

1. Develop a system-level continuous monitoring strategy and implement continuous monitoring by the organisation-level continuous monitoring strategy that includes:

2. Establishing the following system-level metrics to be monitored: [organisation- defined system-level metrics];

3. Establishing [organisation-defined frequencies] for monitoring and [organisation-defined frequencies] for assessment of control effectiveness;

4. Ongoing control assessments by the continuous monitoring strategy;

5. Ongoing monitoring of system and organisation-defined metrics by the continuous monitoring strategy;

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

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

8. Reporting the security and privacy status of the system to [organisation-defined personnel or roles] [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

SAA-7 (4) CONTINUOUS MONITORING | RISK MONITORING

CONTROL DESCRIPTION

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

    i. Effectiveness monitoring;
    ii. Compliance monitoring; and
    iii. Change monitoring.

IMPLEMENTATION DETAILS

Reference the control description above.

SAA-8 | PENETRATION TESTING

CONTROL DESCRIPTION

Conduct penetration testing [organisation-defined frequency] on [organisation-defined systems or system components].

IMPLEMENTATION DETAILS

Each SAI implements an Internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information to subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test.

SAA-9 | INTERNAL SYSTEM CONNECTIONS

CONTROL DESCRIPTION

1. Authorise internal connections of [organisation-defined system components or classes of components] to the system;

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

3. Terminate internal system connections after [organisation-defined conditions]; and

4. Review [organisation-defined frequency] the continued need for each internal connection.

IMPLEMENTATION DETAILS

Reference the control description above.

CM – CONFIGURATION MANAGEMENT

CM-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to [organisation-defined personnel or roles]:

    i. [Select (one or more): organisation-level; mission/business process-level; system-level] configuration management policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and
    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

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

2. Designate an [organisation-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and

3. Review and update the current configuration management:

    i. Policy [organisation-defined frequency]; and
    ii. Procedures [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

CM-2 | BASELINE CONFIGURATION

CONTROL DESCRIPTION

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

2. Review and update the baseline configuration of the system:

    i. [organisation-defined frequency];
    ii. When required due to [Assignment organisation-defined circumstances]; and.
    iii. When system components are installed or upgraded.

IMPLEMENTATION DETAILS

Reference the control description above.

CM-4 | IMPACT ANALYSES

CONTROL DESCRIPTION

Analyse changes to the system to determine potential security and privacy impacts before change implementation.

IMPLEMENTATION DETAILS

The information owner shall approve all security-related information resource changes through a change control process.

Approval shall occur before implementation by the SAI or independent contractors.

CM-5 | ACCESS RESTRICTIONS FOR CHANGE

CONTROL DESCRIPTION

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

IMPLEMENTATION DETAILS

Reference the control description above.

CM-6 | CONFIGURATION SETTINGS

CONTROL DESCRIPTION

1. Establish and document configuration settings for components employed within the system using [organisation-defined common secure configurations] that reflect the most restrictive mode consistent with operational requirements;

2. Implement the configuration settings;

3. Identify, document, and approve any deviations from established configuration settings for [organisation-defined system components] based on [organisation-defined operational requirements]; and

4. Monitor and control changes to the configuration settings by organisational policies and procedures.

IMPLEMENTATION DETAILS

Reference the control description above.

CM-7 | LEAST FUNCTIONALITY

CONTROL DESCRIPTION

1. Configure the system to provide only [organisation-defined mission essential capabilities]; and

2. Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [organisation-defined prohibited or restricted functions, ports, protocols, software, and/or services].

IMPLEMENTATION DETAILS

Reference the control description above.

CM-8 | SYSTEM COMPONENT INVENTORY

CONTROL DESCRIPTION

1. Develop and document an inventory of system components that:

    i. Accurately reflects the system;

    ii. Includes all components within the system;

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

    iv. Includes the following information to achieve system component accountability: [organisation-defined information deemed necessary to achieve effective system component accountability]; and

2. Review and update the system component inventory [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

CM-8 | SYSTEM COMPONENT INVENTORY

CONTROL DESCRIPTION

1. Use software and associated documentation by contract agreements and copyright laws;

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

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

IMPLEMENTATION DETAILS

Reference the control description above.

CM-11 | USER-INSTALLED SOFTWARE

CONTROL DESCRIPTION

1. Establish [organisation-defined policies] governing the installation of software by users;

2. Enforce software installation policies through the following methods: [organisation-defined methods]; and

3. Monitor policy compliance [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

CP – CONTINGENCY PLANNING

CP-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to [organisation-defined personnel or roles]:

    i. [Select (one or more): organisation-level; mission/business process-level; system- level] contingency planning policy that:

        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and
        - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

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

2. Designate an [organisation-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and

3. Review and update the current contingency planning:

    i. Policy [organisation-defined frequency]; and
    ii. Procedures [organisation-defined frequency].

IMPLEMENTATION DETAILS

SAIs shall maintain written Continuity of Operations Plans that address information resources so that the effects of a disaster will be minimised and the SAI can either maintain or quickly resume mission-critical functions.

CP-2 | CONTINGENCY PLAN

CONTROL DESCRIPTION

1. Develop a contingency plan for the system that:

    i. Identifies essential missions and business functions and associated contingency requirements;

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

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

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

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

    v. Is reviewed and approved by [organisation-defined personnel or roles];

2. Distribute copies of the contingency plan to [organisation-defined key contingency personnel (identified by name and/or by role) and organisational elements];

3. Coordinate contingency planning activities with incident handling activities;

4. Review the contingency plan for the system [organisation-defined frequency];

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

6. Communicate contingency plan changes to organisation-defined key contingency personnel (identified by name and/or by role) and [organisational elements]; and

7. Protect the contingency plan from unauthorised disclosure and modification.

IMPLEMENTATION DETAILS

The plan shall be distributed to key personnel, and a copy will be stored off-site. Elements of the plan for information resources shall include:

1. a. Business Impact Analysis to systematically assess the potential impacts of a loss of business functionality due to an interruption of computing and/or infrastructure support services resulting from various events or incidents. The analysis shall identify the following elements:

    i. Mission-critical information resources (specific system resources required to perform critical functions) include:

        - Internal and external points of contact for personnel that provide or receive data or support interconnected systems.

        - Supporting infrastructure such as electric power, telecommunications connections, and environmental controls.

    ii. Disruption impacts and allowable outage times include:

        - Effects of an outage over time to assess the maximum allowable time that a resource may be denied before it prevents or inhibits the performance of an essential function.

        - Effects of an outage across related resources and dependent systems to assess cascading effects on associated systems or processes.

    iii. Recovery priorities that consider geographic areas, accessibility, security, environment, and cost and may include a combination of:

        - Preventative controls and processes include backup power, excess capacity, environmental sensors and alarms.

- Recovery techniques and technologies include backup methodologies, alternate sites, software and hardware equipment replacement, implementation roles and responsibilities.

2. b. Risk Assessment to weigh the cost of implementing preventative measures against the risk of loss from not taking action.

3. c. Implementation, testing, and maintenance management programme addressing the plan's initial and ongoing testing and maintenance activities.

4. d. Disaster Recovery Plan: Each SAI shall maintain a written disaster recovery plan for major or catastrophic events that deny access to information resources for an extended period. Information learned from tests conducted since the plan was last updated will be used in updating the disaster recovery plan. The disaster recovery plan will:

    i. Contain measures which address the impact and magnitude of loss or harm that will result from an interruption;
    ii. Identify recovery resources and a source for each;
    iii. Contain step-by-step implementation instructions; and
    iv. Include provisions for annual testing.

CP-3 | CONTINGENCY TRAINING

CONTROL DESCRIPTION

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

    i. Within [organisation-defined time-period] of assuming a contingency role or responsibility;
    ii. When required by system changes; and
    iii. [organisation-defined frequency] thereafter.

IMPLEMENTATION DETAILS

Reference the control description above.

CP-4 | CONTINGENCY PLAN TESTING

CONTROL DESCRIPTION

1. Test the contingency plan for the system [organisation-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [organisation-defined tests].

2. Review the contingency plan test results; and c. Initiate corrective actions if needed.

IMPLEMENTATION DETAILS

Each SAI's written disaster recovery plan shall include provisions for annual testing.

CP-6 | ALTERNATE STORAGE SITE

CONTROL DESCRIPTION

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

2. Ensure the alternate storage site provides controls equivalent to the primary site's.

IMPLEMENTATION DETAILS

Mission-critical information shall be backed up on a scheduled basis and stored off-site in a secure, environmentally safe, locked facility accessible only to authorised SAI representatives.

CP-9 | SYSTEM BACKUP

CONTROL DESCRIPTION

1. Conduct backups of user-level information contained in [organisation-defined system components] [organisation-defined frequency consistent with recovery time and recovery point objectives];

2. Conduct backups of system-level information contained in the system [organisation-defined frequency consistent with recovery time and recovery point objectives];

3. Conduct backups of system documentation, including security and privacy-related documentation [organisation-defined frequency consistent with recovery time and recovery point objectives]; and

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

IMPLEMENTATION DETAILS

Reference the control description above.

CP-10 | SYSTEM RECOVERY AND RECONSTITUTION

CONTROL DESCRIPTION

Provide for the recovery and reconstitution of the system to a known within [organisation-defined time-period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.

IMPLEMENTATION DETAILS

Reference the control description above.

CP-11 | ALTERNATE COMMUNICATIONS PROTOCOLS

CONTROL DESCRIPTION

Provide the capability to employ [organisation-defined alternative communications protocols] to maintain continuity of operations.

IMPLEMENTATION DETAILS

Reference the control description above.

IA – IDENTIFICATION AND AUTHENTICATION

IA-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to [organisation-defined personnel or roles]:

    i. An identification and authentication policy that:

        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and
        - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

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

2. Designate an [organisation-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and

3. Review and update the current identification and authentication:

    i. Policy [organisation-defined frequency]; and
    ii. Procedures [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

IA-2 | IDENTIFICATION AND AUTHENTICATION (ORGANISATIONAL USERS)

CONTROL DESCRIPTION

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

IMPLEMENTATION DETAILS

Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resources system may grant that user access.

IA-2 (1) | MULTIFACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS

CONTROL DESCRIPTION

Implement multifactor authentication for access to privileged accounts for [organisation-defined information systems or system categorisations].

IMPLEMENTATION DETAILS

Reference the control description above.

IA-2 (2) | MULTIFACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS

CONTROL DESCRIPTION

Implement multifactor authentication to access non-privileged accounts for select [organisation-defined systems].

IMPLEMENTATION DETAILS

Reference the control description above.

IA-4 | IDENTIFIER MANAGEMENT

CONTROL DESCRIPTION

Manage system identifiers by:

1. Receiving authorisation from [organisation-defined personnel or roles] to assign an individual, group, role, service, or device identifier;

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

3. Assigning the identifier to the intended individual, group, role, service, or device; and d. Preventing reuse of identifiers for [organisation-defined time-period].

IMPLEMENTATION DETAILS

A user's access authorisation shall be appropriately modified or removed when the user's employment or job responsibilities within the SAI change.

IA-5 | AUTHENTICATOR MANAGEMENT

CONTROL DESCRIPTION

Manage system authenticators by:

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

2. Establishing initial authenticator content for any authenticators issued by the organisation;

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

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

5. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

6. Changing default authenticators before first use;

7. Changing or refreshing authenticators [organisation-defined time-period by authenticator type];

8. Protecting authenticator content from unauthorised disclosure and modification;

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

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

IMPLEMENTATION DETAILS

Reference the control description above.

IA-6 | AUTHENTICATOR FEEDBACK

CONTROL DESCRIPTION

Obscure feedback on authentication information during the authentication process to protect the information from possible exploitation and use by unauthorised individuals.

IMPLEMENTATION DETAILS

Reference the control description above.

IA-7 | CRYPTOGRAPHIC MODULE AUTHENTICATION

CONTROL DESCRIPTION

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

IMPLEMENTATION DETAILS

Reference the control description above.

IA-8 | IDENTIFICATION AND AUTHENTICATION (NON-ORGANISATIONAL USERS)

CONTROL DESCRIPTION

Uniquely identify and authenticate non-organisational users or processes acting for non-organisational users.

IMPLEMENTATION DETAILS

Reference the control description above.

IA-11 | RE-AUTHENTICATION

CONTROL DESCRIPTION

Require users to re-authenticate when [organisation-defined circumstances or situations requiring re-authentication].

IMPLEMENTATION DETAILS

Reference the control description above.

IR – INCIDENT RESPONSE

IR-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to [organisation-defined personnel or roles]:

    i. An incident response policy that:
        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and
        - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

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

2. Designate an [organisation-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and

3. Review and update the current incident response:

        i. Policy [organisation-defined frequency]; and
        ii. Procedures [organisation-defined frequency].

IMPLEMENTATION DETAILS

SAIs shall assess the significance of a security incident based on the business impact on the affected resources and the incident's current and potential technical effect, for example, loss of revenue, productivity, access to services, reputation, unauthorised disclosure of confidential information, or propagation to other networks.

IR-2 | INCIDENT RESPONSE TRAINING

CONTROL DESCRIPTION

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

i. Within [organisation-defined time-period] of assuming an incident response role or responsibility or acquiring system access;

ii. When required by system changes; and

iii. [organisation-defined frequency] thereafter.

IMPLEMENTATION DETAILS

The SAI trains personnel in their incident response roles and responsibilities concerning the information system and provides refresher training at least annually.

IR-3 | INCIDENT RESPONSE TESTING

CONTROL DESCRIPTION

Test the effectiveness of the incident response capability for the system [organisation-defined frequency] using the following tests: [organisation-defined tests].

IMPLEMENTATION DETAILS

Reference the control description above.

IR-4 | INCIDENT HANDLING

CONTROL DESCRIPTION

1. 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;

2. Coordinate incident handling activities with contingency planning activities;

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

4. Ensure the rigour, intensity, scope, and results of incident handling activities are comparable and predictable across the organisation.

IMPLEMENTATION DETAILS

Reference the control description above.

IR-5 | INCIDENT MONITORING

CONTROL DESCRIPTION

Track and document security, privacy, and supply chain incidents.

IMPLEMENTATION DETAILS

Reference the control description above.

IR-6 | INCIDENT REPORTING

CONTROL DESCRIPTION

1. Require personnel to report suspected security, privacy, and supply chain incidents to the organisational incident response capability within [organisation-defined time-period]; and

2. Report security, privacy, and supply chain incident information to [organisation-defined authorities].

IMPLEMENTATION DETAILS

Reporting of security incidents and the investigation and restoration of operations following a security incident assessed to involve suspected criminal activity shall comply with local legislation.

IR-7 | INCIDENT RESPONSE ASSISTANCE

CONTROL DESCRIPTION

Provide an incident response support resource, integral to the organisational incident response capability, that offers advice and assistance to system users for handling and reporting security, privacy, and supply chain incidents.

IMPLEMENTATION DETAILS

The SAI provides an incident response support resource that offers advice and assistance to information system users for handling and reporting security incidents. The support resource is integral to the SAI's incident response capability.

IR-8 | INCIDENT RESPONSE PLAN

CONTROL DESCRIPTION

1. Develop an incident response plan that:
   i. Provides the organisation with a roadmap for implementing its incident response capability;
   ii. Describes the structure and organisation of the incident response capability;
   i. Provides a high-level approach for how the incident response capability fits into the overall organisation;
   ii. Meets the unique requirements of the organisation, which relate to mission, size, structure, and functions;
   iii. Defines reportable incidents;
   iv. Provides metrics for measuring the incident response capability within the organisation;
   v. Defines the resources and management support needed to maintain and mature an incident response capability effectively;
   vi. Is reviewed and approved by [organisation-defined personnel or roles] [organisation-defined frequency]; and
   vii. Explicitly designates responsibility for incident response to [organisation-defined entities, personnel or roles].

2. Distribute copies of the incident response plan to [organisation-defined incident response personnel (identified by name and/or by role) and organisational elements];

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

4. Communicate incident response plan changes to [organisation-defined incident response personnel (identified by name and/or by role) and organisational elements]; and

5. Protect the incident response plan from unauthorised disclosure and modification.

IMPLEMENTATION DETAILS

Reference the control description above.

IR-9 | INFORMATION SPILLAGE RESPONSE

CONTROL DESCRIPTION

Respond to information spills by:

1. Assigning [organisation-defined personnel or roles] with responsibility for responding to information spills;

2. Identifying the specific information involved in the system contamination;

3. Alerting [organisation-defined personnel or roles] of the information spill using a method of communication not associated with the spill;

4. Isolating the contaminated system or system component;

5. Eradicating the information from the contaminated system or component;

6. Identifying other systems or system components that may have been subsequently contaminated; and

7. Performing the following additional actions: [organisation-defined actions].

IMPLEMENTATION DETAILS

Reference the control description above.

MA – MAINTENANCE

MA-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to [organisation-defined personnel or roles]:

    i. A maintenance policy that:
    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and
    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

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

2. Designate an [organisation-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and

3. Review and update the current maintenance:

    i. Policy [organisation-defined frequency]; and
    ii. Procedures [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

MA-2 | CONTROLLED MAINTENANCE

CONTROL DESCRIPTION

1. Schedule, document, and review records of maintenance, repair, or replacement of system components by manufacturer or vendor specifications and/or organisational requirements;

2. 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;

3. Require that [organisation-defined personnel or roles] explicitly approve the removal of the system or system components from organisational facilities for off-site maintenance, repair, or replacement;

4. Sanitise equipment to remove the following information from associated media before removal from organisational facilities for off-site maintenance, repair, or replacement: [organisation-defined information];

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

6. Include the following information in organisational maintenance records: [organisation-defined information].

IMPLEMENTATION DETAILS

Reference the control description above.

MA-4 | NONLOCAL MAINTENANCE

CONTROL DESCRIPTION

1. Approve and monitor nonlocal maintenance and diagnostic activities;

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

3. Employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions;

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

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

IMPLEMENTATION DETAILS

Reference the control description above.

MA-5 | MAINTENANCE PERSONNEL

CONTROL DESCRIPTION

1. Establish a process for maintenance personnel authorisation and maintain a list of authorised maintenance organisations or personnel;

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

3. Designate organisational personnel with required access authorisations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorisations.

IMPLEMENTATION DETAILS

Reference the control description above.

MP – MEDIA PROTECTION

MP-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to [organisation-defined personnel or roles]:

    i. [Select (one or more): organisation-level; mission/business process-level; system- level] media protection policy that:
        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and
        - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

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

2. Designate an [organisation-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; and

3. Review and update the current media protection:

    i. Policy [organisation-defined frequency]; and
    ii. Procedures [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

MP-2 | MEDIA ACCESS

CONTROL DESCRIPTION

Restrict access to [organisation-defined types of digital and/or non-digital media] to [organisation-defined personnel or roles].

IMPLEMENTATION DETAILS

Reference the control description above.

MP-6 | MEDIA SANITISATION

CONTROL DESCRIPTION

1. Sanitise [organisation-defined system media] before disposal, release out of organisational control, or release for reuse using [organisation-defined sanitisation techniques and procedures]; and

2. Employ sanitisation mechanisms with the strength and integrity commensurate with the security category or classification of the information.

IMPLEMENTATION DETAILS

Before transferring data processing equipment to any party other than the other, SAIs shall assess whether to remove data from any associated storage device.

Electronic records shall be destroyed in accordance and compliance with the SAI's records retention schedule. If the record retention period applicable for an electronic record has not expired when the record is removed from data process equipment, the SAI shall retain a hard copy or other electronic copy of the record for the required retention period.

If restricted personal information, confidential information, mission-critical information, intellectual property, or licensed software may be contained on the storage device, the storage device should be sanitised or the storage device should be removed and destroyed.

SAIs shall keep a record/form (electronic or hard copy) documenting the removal and completion of the process with the following information:

- date;
- description of the item(s) and serial number(s);
- inventory number(s);
- the process and sanitisation tools used to remove the data or method of destruction; and
- the name and address of the organisation to which the equipment was transferred.

MP-7 | MEDIA USE

CONTROL DESCRIPTION

1. [Select: Restrict; Prohibit] the use of [organisation-defined types of system media] on [organisation-defined systems or system components] using [organisation-defined controls]; and

2. Prohibit portable storage devices in organisational systems when such devices have no identifiable owner.

IMPLEMENTATION DETAILS

Reference the control description above.

PE – PHYSICAL AND ENVIRONMENTAL PROTECTION

PE-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to [organisation-defined personnel or roles]:

    i. [Select (one or more)]: organisation-level; mission/business process-level; system-level] physical and environmental protection policy that:

    - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and
    - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

    ii. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;

2. Designate an [organisation-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and

3. Review and update the current physical and environmental protection:

    i. Policy [organisation-defined frequency]; and
    ii. Procedures [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

PE-2 | PHYSICAL ACCESS AUTHORISATIONS

CONTROL DESCRIPTION

1. Define and document all physical assets within the SAI, categorising them based on type, value, criticality, and location.
2. Develop, approve, and maintain a list of individuals with authorised access to the facility where the system resides.
3. Issue authorisation credentials for facility access.
4. Review the access list detailing authorised facility access by individuals [organisation-defined frequency].
5. Remove individuals from the facility access list when access is no longer required.

IMPLEMENTATION DETAILS

Reference the control description above.

PE-3 | PHYSICAL ACCESS CONTROL

CONTROL DESCRIPTION

1. Enforce physical access authorisations at [organisation-defined entry and exit points to the facility where the system resides] by:

    i. Verifying individual access authorisations before granting access to the facility; and

    ii. Controlling ingress and egress to the facility using [Select (one or more)]: [organisation-defined physical access control systems or devices or guards];

1. Maintain physical access audit logs for [organisation-defined entry or exit points];

2. Control access to areas within the facility designated as publicly accessible by implementing the following controls: [organisation-defined controls];

3. Escort visitors and monitor visitor activity [organisation-defined circumstances requiring visitor escorts and monitoring];

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

5. Inventory [organisation-defined physical access devices] every [organisation-defined frequency]; and

6. Change combinations and keys [organisation-defined frequency] and/or when keys are lost, combinations are compromised, individuals possessing the keys or combinations are transferred, or employment is terminated.

IMPLEMENTATION DETAILS

Reference the control description above.

PE-6 | MONITORING PHYSICAL ACCESS

CONTROL DESCRIPTION

1. Monitor physical access to the system's facility to detect and respond to physical security incidents.

2. Review physical access logs [organisation-defined frequency] and upon occurrence of [organisation-defined events or potential indications of events]; and

3. Coordinate results of reviews and investigations with the organisational incident response capability.

IMPLEMENTATION DETAILS

Reference the control description above.

PE-8 | VISITOR ACCESS RECORDS

CONTROL DESCRIPTION

1. Maintain visitor access records to the facility where the system resides for [organisation-defined time-period];

2. Review visitor access records [organisation-defined frequency]; and

3. Report anomalies in visitor access records to [organisation-defined personnel].

IMPLEMENTATION DETAILS

Reference the control description above.

PE-12 | EMERGENCY LIGHTING

CONTROL DESCRIPTION

Employ and maintain automatic emergency lighting for the system that activates during a power outage or disruption and covers emergency exits and evacuation routes within the facility.

IMPLEMENTATION DETAILS

Reference the control description above.

PE-13 | FIRE PROTECTION

CONTROL DESCRIPTION

Employ and maintain fire detection and suppression systems supported by an independent energy source.

IMPLEMENTATION DETAILS

Information resources shall be protected from environmental hazards. Designated employees shall be trained to monitor environmental control procedures and equipment and shall be trained in desired response in case of emergencies or equipment problems.

PE-14 | ENVIRONMENTAL CONTROLS

CONTROL DESCRIPTION

1. Maintain [Select (one or more)]: temperature, humidity, pressure, radiation, [organisation-defined environmental control] levels within the facility where the system resides at [organisation-defined acceptable levels]; and

2. Monitor environmental control levels [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

PE-15 | WATER DAMAGE PROTECTION

CONTROL DESCRIPTION

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.

IMPLEMENTATION DETAILS

Reference the control description above.

PE-16 | DELIVERY AND REMOVAL

CONTROL DESCRIPTION

1. Authorise and control [organisation-defined types of system components] entering and exiting the facility; and

2. Maintain records of the system components.

IMPLEMENTATION DETAILS

Reference the control description above.

PE-17 | ALTERNATE WORK SITE

CONTROL DESCRIPTION

1. Determine and document the [organisation-defined alternate work sites] allowed for use by employees;

2. Employ the following controls at alternate work sites: [organisation-defined controls];

3. Assess the effectiveness of controls at alternate work sites; and

4. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

IMPLEMENTATION DETAILS

Reference the control description above.

PL – PLANNING

PL-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to [organisation-defined personnel or roles]:

    i. [Select (one or more)]: organisation-level; mission/business process-level; system-level] planning policy that:

        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and
        - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

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

2. Designate an [organisation-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; and

3. Review and update the current planning:

    i. Policy [organisation-defined frequency]; and
    ii. Procedures [organisation-defined frequency].

IMPLEMENTATION DETAILS

The SAI information security officer reports annually on the SAI information security programme.

PL-2 | SYSTEM SECURITY AND PRIVACY PLANS

CONTROL DESCRIPTION

1. Develop security and privacy plans for the system that:

    i. Are consistent with the organisation's enterprise architecture;
    ii. Explicitly define the constituent system components;
    iii. Describe the operational context of the system in terms of missions and business processes;
    iv. Provide the security categorisation of the system, including supporting rationale;
    v. Describe any specific threats to the system that are of concern to the organisation;
    vi. Provide the results of a privacy risk assessment for systems processing personally identifiable information;
    vii. Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
    viii. Provide an overview of the security and privacy requirements for the system;
    ix. Identify any relevant control baselines or overlays, if applicable;
    x. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
    xi. Include risk determinations for security and privacy architecture and design decisions;
    xii. Include security- and privacy-related activities affecting the system that require planning and coordination with [organisation-defined individuals or groups]; and
    xiii. Are reviewed and approved by the authorising official or designated representative before plan implementation.

2. Distribute copies of the plans and communicate subsequent changes to the plans to [organisation-defined personnel or roles];

3. Review the plans [organisation-defined frequency];

4. Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and

5. Protect the plans from unauthorised disclosure and modification.

IMPLEMENTATION DETAILS

Reference the control description above.

PL-4 | RULES OF BEHAVIOUR

CONTROL DESCRIPTION

1. Establish and provide to individuals requiring access to the system the rules that describe their responsibilities and expected behaviour for information and system usage, security, and privacy;

2. Receive a documented acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behaviour before authorising access to information and the system;

3. Review and update the rules of behaviour [organisation-defined frequency]; and

4. Require individuals who have acknowledged a previous version of the rules of behaviour to read and re-acknowledge [Select (one or more)]: [organisation-defined frequency]; [when the rules are revised or updated].

IMPLEMENTATION DETAILS

Reference the control description above.

PM – PROGRAMME MANAGEMENT

PM-1 | INFORMATION SECURITY PROGRAMME PLAN

CONTROL DESCRIPTION

1. Develop and disseminate an organisation-wide information security programme plan that:

    i. Provides an overview of the requirements for the security programme and a description of the security programme management controls and common controls in place or planned for meeting those requirements;

    ii. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organisational entities, and compliance;

    iii. Reflects the coordination among organisational entities responsible for information security; and

    iv. Is approved by a senior official with responsibility and accountability for the risk being incurred to organisational operations (including mission, functions, image, and reputation), organisational assets, individuals, other organisations, and the Nation;

2. Review the organisation-wide information security programme plan [organisation-defined frequency];

3. Update the information security programme plan to address organisational changes and problems identified during plan implementation or control assessments; and

4. Protect the information security programme plan from unauthorised disclosure and modification.

IMPLEMENTATION DETAILS

Reference the control description above.

PM-2 | INFORMATION SECURITY PROGRAMME LEADERSHIP ROLE

CONTROL DESCRIPTION

Appoint a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organisation-wide information security programme.

IMPLEMENTATION DETAILS

Reference the control description above.

PM-3 | INFORMATION SECURITY AND PRIVACY RESOURCES

CONTROL DESCRIPTION

1. Include the resources needed to implement the information security and privacy programmes in capital planning and investment requests and document all exceptions to this requirement;

2. Prepare documentation required for addressing information security and privacy programmes in capital planning and investment requests by applicable laws, executive orders, directives, policies, regulations, standards; and

3. Make the planned information security and privacy resources available for expenditure.

IMPLEMENTATION DETAILS

Reference the control description above.

PM-4 | PLAN OF ACTION AND MILESTONES PROCESS

CONTROL DESCRIPTION

1. Implement a process to ensure that plans of action and milestones for the information security and privacy programmes and associated organisational systems:

    i. Are developed and maintained;

    ii. Document the remedial information security and privacy actions to adequately respond to risk to organisational operations and assets, individuals, other organisations, the of Texas, and the Nation; and

    iii. Are reported by established reporting requirements.

2. Review action plans and milestones for consistency with the organisational risk management strategy and organisation-wide priorities for risk response actions.

IMPLEMENTATION DETAILS

Reference the control description above.

PM-5 | SYSTEM INVENTORY

CONTROL DESCRIPTION

Develop and update [organisation-defined frequency] an inventory of organisational systems.

IMPLEMENTATION DETAILS

Reference the control description above.

PM-6 | MEASURES OF PERFORMANCE

CONTROL DESCRIPTION

Develop, monitor, and report on the results of information security and privacy measures of performance.

IMPLEMENTATION DETAILS

Reference the control description above.

PM-7 | ENTERPRISE ARCHITECTURE

CONTROL DESCRIPTION

Develop and maintain an enterprise architecture considering information security, privacy, and risk to organisational operations and assets, individuals, other organisations, the state of Texas, and the Nation.

IMPLEMENTATION DETAILS

Reference the control description above.

PM-9 | RISK MANAGEMENT STRATEGY

CONTROL DESCRIPTION

1. Develops a comprehensive strategy to manage:

    i. Security risk to organisational operations and assets, individuals, organisations, etc. associated with the operation and use of organisational systems; and

    ii. Privacy risk to individuals resulting from the authorised processing of personally identifiable information;

2. Implement the risk management strategy consistently across the organisation; and

3. Review and update the risk management strategy [organisation-defined frequency] or, as required, to address organisational changes.

IMPLEMENTATION DETAILS

Reference the control description above.

PM-10 | AUTHORISATION PROCESS

CONTROL DESCRIPTION

1. Manage the security and privacy of organisational systems and the environments in which those systems operate through authorisation processes;

2. Designate individuals to fulfil specific roles and responsibilities within the organisational risk management process; and

3. Integrate the authorisation processes into an organisation-wide risk management programme.

IMPLEMENTATION DETAILS

Reference the control description above.

PM-14 | TESTING, TRAINING, AND MONITORING

CONTROL DESCRIPTION

1. Implement a process for ensuring that organisational plans for conducting security and privacy testing, training, and monitoring activities associated with organisational systems:

    i. Are developed and maintained; and
    ii. Continue to be executed; and

2. Review testing, training, and monitoring plans for consistency with the organisational risk management strategy and organisation-wide priorities for risk response actions.

IMPLEMENTATION DETAILS

Reference the control description above.

PM-15 | SECURITY AND PRIVACY GROUPS AND ASSOCIATIONS

CONTROL DESCRIPTION

Establish and institutionalise contact with selected groups and associations within the security and privacy communities:

i. To facilitate ongoing security and privacy education and training for organisational personnel;

ii. To maintain currency with recommended security and privacy practices, techniques, and technologies; and

iii. To share security and privacy information, including threats, vulnerabilities, and incidents.

IMPLEMENTATION DETAILS

Reference the control description above.

PM-16 | THREAT AWARENESS PROGRAMME

CONTROL DESCRIPTION

Implement a threat awareness programme with a cross-organisation information-sharing capability for threat intelligence.

IMPLEMENTATION DETAILS

Reference the control description above.

PS – PERSONNEL SECURITY

PS-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to [organisation-defined personnel or roles]:

    i. [Select (one or more): organisation-level; mission/business process-level; system-level] personnel security policy that:

        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and

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

    ii. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;

2. Designate an [organisation-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and

3. Review and update the current personnel security:

    i. Policy [organisation-defined frequency]; and

    ii. Procedures [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

PS-2 | POSITION RISK DESIGNATION

CONTROL DESCRIPTION

1. Assign a risk designation to all organisational positions;

2. Establish screening criteria for individuals filling those positions; and

3. Review and update position risk designations [organisation-defined frequency].

IMPLEMENTATION DETAILS

All authorised users (including, but not limited to, SAI personnel, temporary employees, and employees of independent contractors) of the SAI's information resources shall formally acknowledge that they will comply with the security policies and procedures of the SAI or they shall not be granted access to information resources. The SAI head or their designated representative will determine the method of acknowledgement and how often this acknowledgement must be re-executed by the user to maintain access to SAI information resources.

PS-3 | PERSONNEL SCREENING

CONTROL DESCRIPTION

1. Screen individuals before authorising access to the system; and

2. Rescreen individuals by [organisation-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening].

IMPLEMENTATION DETAILS

Reference the control description above.

PS-4 | PERSONNEL TERMINATION

CONTROL DESCRIPTION

Upon termination of individual employment:

i. Disable system access within [organisation-defined time-period];

ii. Terminate or revoke any authenticators and credentials associated with the individual;

iii. Conduct exit interviews that include a discussion of [organisation-defined information security topics];

iv. Retrieve all security-related organisational system-related property; and

v. Retain access to organisational information and systems formerly controlled by terminated individuals.

IMPLEMENTATION DETAILS

Reference the control description above.

PS-5 | PERSONNEL TRANSFER

CONTROL DESCRIPTION

1. Review and confirm ongoing operational need for current logical and physical access authorisations to systems and facilities when individuals are reassigned or transferred to other positions within the organisation;

2. Initiate [organisation-defined transfer or reassignment actions] within [organisation-defined time-period following the formal transfer action];

3. Modify access authorisation as needed to correspond with any changes in operational need due to reassignment or transfer; and

4. Notify [organisation-defined personnel or roles] within [organisation-defined time-period].

IMPLEMENTATION DETAILS Reference the control description above.

PS-6 | ACCESS AGREEMENTS

CONTROL DESCRIPTION

1. Develop and document access agreements for organisational systems;

2. Review and update the access agreements [organisation-defined frequency]; and c. Verify that individuals requiring access to organisational information and systems:

    i. Sign appropriate access agreements before being granted access; and
    ii. Re-sign access agreements to maintain access to organisational systems when access agreements have been updated or [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

PS-7 | EXTERNAL PERSONNEL SECURITY

CONTROL DESCRIPTION

1. Establish personnel security requirements, including security roles and responsibilities for external providers;

2. Require external providers to comply with personnel security policies and procedures established by the organisation;

3. Document personnel security requirements;

4. Require external providers to notify [organisation-defined personnel or roles] of any personnel transfers or terminations of external personnel who possess organisational credentials and/or badges or who have system privileges within [organisation-defined time-period]; and

5. Monitor provider compliance with personnel security requirements.

IMPLEMENTATION DETAILS

Reference the control description above.

PS-8 | PERSONNEL SANCTIONS

CONTROL DESCRIPTION

1. Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and

2. Notify [organisation-defined personnel or roles] within [organisation-defined time-period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.

IMPLEMENTATION DETAILS

Reference the control description above.

RA – RISK ASSESSMENT

RA-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to [organisation-defined personnel or roles]:

    i. Select (one or more): organisation-level; mission/business process-level; system-level] risk assessment policy that:

        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and
        - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

    ii. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;

2. Designate an [organisation-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and

3. Review and update the current risk assessment:

    i. Policy [organisation-defined frequency]; and
    ii. Procedures [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

RA-2 | SECURITY CATEGORISATION

CONTROL DESCRIPTION

1. Categorise the system and the information it processes, stores, and transmits;

2. Document the security categorisation results, including supporting rationale, in the security plan for the system; and

3. Verify that the authorising official or authorising official designated representative reviews and approves the security categorisation decision.

IMPLEMENTATION DETAILS

SAIs are responsible for identifying and defining all information classification categories and establishing the appropriate controls for each.

RA-3 | RISK ASSESSMENT

CONTROL DESCRIPTION

1. Conduct a risk assessment, including:

    i. The likelihood and magnitude of harm from unauthorised access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and

    ii. The likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;

2. Integrate risk assessment results and risk management decisions from the organisation and mission or business process perspectives with system-level risk assessments;

3. Document risk assessment results in [Select: security and privacy plans; risk assessment report; [organisation-defined document]];

4. Review risk assessment results [organisation-defined frequency];

5. Disseminate risk assessment results to [organisation-defined personnel or roles]; and

6. Update the risk assessment [organisation-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy of the system.

IMPLEMENTATION DETAILS

The SAI shall perform and document risk assessments and make and document risk management decisions in compliance with the organisation-wide risk framework.

RA-3 (1) | SUPPLY CHAIN RISK ASSESSMENT

CONTROL DESCRIPTION

1. Assess supply chain risks associated with [organisation-defined systems, system components, and system services]; and

2. Update the supply chain risk assessment [organisation-defined frequency] 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.

IMPLEMENTATION DETAILS

Reference the control description above.

RA-5 | VULNERABILITY MONITORING AND SCANNING

CONTROL DESCRIPTION

1. Monitor and scan for vulnerabilities in the system and hosted applications [organisation-defined frequency and/or randomly by organisation-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;

2. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

    i. Enumerating platforms, software flaws, and improper configurations;

    ii. Formatting checklists and test procedures; and

    iii. Measuring vulnerability impact;

3. Analyse vulnerability scan reports and results from vulnerability monitoring;

4. Remediate legitimate vulnerabilities [organisation-defined response times] by an organisational assessment of risk;

5. Share information obtained from the vulnerability monitoring process and control assessments with [organisation-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and

6. Employ vulnerability monitoring tools that can readily update the vulnerabilities to be scanned.

IMPLEMENTATION DETAILS

The SAI scans for vulnerabilities in the information system at least annually or when significant new vulnerabilities potentially affecting the system are identified and reported.

RA-7 | RISK RESPONSE

CONTROL DESCRIPTION

Respond to findings from security and privacy assessments, monitoring, and audits by organisational risk tolerance.

IMPLEMENTATION DETAILS

Reference the control description above.

SA – SYSTEM AND SERVICE ACQUISITION

SA-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to [organisation-defined personnel or roles]:

    i. A system and services acquisition policy that:

        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and
        - Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

    i. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;

2. Designate an [organisation-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and

3. Review and update the current system and services acquisition:

    i. Policy [organisation-defined frequency]; and
    ii. Procedures [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

SA-2 | ALLOCATION OF RESOURCES

CONTROL DESCRIPTION

1. Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;

2. Determine, document, and allocate the resources required to protect the system or system service as part of the organisational capital planning and investment control process; and

3. Establish a discrete line item for information security and privacy in organisational programming and budgeting documentation.

IMPLEMENTATION DETAILS

Reference the control description above.

SA-3 | SYSTEM DEVELOPMENT LIFE CYCLE

CONTROL DESCRIPTION

1. Acquire, develop, and manage the system using [organisation-defined system development life cycle] that incorporates information security and privacy considerations;

2. Define and document information security and privacy roles and responsibilities throughout the system development life cycle;

3. Identify individuals having information security and privacy roles and responsibilities; and

4. Integrate the organisational information security and privacy risk management process into system development life cycle activities.

IMPLEMENTATION DETAILS

A SAI shall include information security, security testing, and audit controls in all phases of the system development lifecycle or acquisition process.

SA-4 | ACQUISITION PROCESS

CONTROL DESCRIPTION

Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Select (one or more): standardised contract language; [organisation-defined contract language]] in the acquisition contract for the system, system component, or system service:

1. Security and privacy functional requirements;
2. Strength of mechanism requirements;
3. Security and privacy assurance requirements;
4. Controls needed to satisfy the security and privacy documentation requirements;
5. Requirements for protecting security and privacy documentation;
6. Description of the system development environment and environment in which the system is intended to operate;
7. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and
8. Acceptance criteria.

IMPLEMENTATION DETAILS

Reference the control description above.

SA-5 | SYSTEM DOCUMENTATION

CONTROL DESCRIPTION

1. Obtain administrator documentation for the system, system component, or system service that describes:
    i. Secure configuration, installation, and operation of the system, component, or service;

    ii. Effective use and maintenance of security and privacy functions and mechanisms; and

    iii. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

2. Obtain user documentation for the system, system component, or system service that describes:
    i. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;

    ii. Methods for user interaction, which enables individuals to use the system, component, or service more securely and protect individual privacy; and

    iii. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;

3. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or non-existent and takes [organisation-defined actions] in response;

4. Protect documentation as required by the organisational risk management strategy; and

5. Distribute documentation to [organisation-defined personnel or roles].

IMPLEMENTATION DETAILS

Reference the control description above.

SA-8 | SECURITY AND PRIVACY ENGINEERING PRINCIPLES

CONTROL DESCRIPTION

Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [organisation-defined systems security and privacy engineering principles].

IMPLEMENTATION DETAILS

Reference the control description above.

SA-9 | EXTERNAL SYSTEM SERVICES

CONTROL DESCRIPTION

1. Require that providers of external system services comply with organisational security and privacy requirements and employ the following controls: [organisation-defined controls].

2. Define and document organisational oversight and user roles and responsibilities about external system services; and

3. Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [organisation-defined processes, methods, and techniques].

IMPLEMENTATION DETAILS

Reference the control description above.

SA-10 | DEVELOPER CONFIGURATION MANAGEMENT

CONTROL DESCRIPTION

Require the developer of the system, system component, or system service to:

1. Perform configuration management during system, component, or service [Select (one or more): design; development; implementation; operation; disposal].

2. Document, manage, and control the integrity of changes to [organisation-defined configuration items under configuration management].

3. Implement only organisation-approved changes to the system, component, or service.

4. Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and

5. Track security flaws and flaw resolution within the system, component, or service and report findings to [organisation-defined personnel].

IMPLEMENTATION DETAILS

The information owner shall approve all security-related information resource changes through a change control process. Approval shall occur before implementation by the SAI or independent contractors.

SA-11 | DEVELOPER TESTING AND EVALUATION

CONTROL DESCRIPTION

Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:

1. Develop and implement a plan for ongoing security and privacy assessments.

2. Perform [Select (one or more): unit; integration; system; regression] testing/evaluation [organisation-defined frequency] at [organisation-defined depth and coverage].

3. Produce evidence of executing the assessment plan and the testing and evaluation results.

4. Implement a verifiable flaw remediation process; and e. Correct flaws identified during testing and evaluation.

IMPLEMENTATION DETAILS

Reference the control description above.

SA-22 | UNSUPPORTED SYSTEM COMPONENTS

CONTROL DESCRIPTION

1. Replace system components when support for the components is no longer available from the developer, vendor, manufacturer; or

2. Provide the following options for alternative sources for continued support for unsupported components [Select (one or more): in-house support; [organisation-defined support from external providers]].

IMPLEMENTATION DETAILS

Reference the control description above.

SC – SYSTEM AND COMMUNICATION PROTECTION

SC-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to [organisation-defined personnel or roles]:

    i. [Select (one or more): organisation-level; mission/business process-level; system-level] system and communications protection policy that:

        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and

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

    ii. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls.

2. Designate an [organisation-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and

3. Review and update the current system and communications protection:

    i. Policy [organisation-defined frequency]; and
    ii. Procedures [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

SC-5 | DENIAL-OF-SERVICE PROTECTION

CONTROL DESCRIPTION

1. [Select: protect against; limit] the effects of the following types of denial-of-service events: [organisation-defined types of denial-of-service events]; and

2. Employ the following controls to achieve the denial-of-service objective: [organisation-defined controls by type of denial-of-service event].

IMPLEMENTATION DETAILS

Reference the control description above.

SC-7 | BOUNDARY PROTECTION

CONTROL DESCRIPTION

1. Monitor and control communications at the system's external interfaces and key internal interfaces within the system.

2. Implement subnetworks for publicly accessible system components that are [Select: physically; logically] separated from internal organisational networks; and

3. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged by an organisational security and privacy architecture.

IMPLEMENTATION DETAILS

Reference the control description above.

SC-8 | TRANSMISSION, CONFIDENTIALITY AND INTEGRITY

CONTROL DESCRIPTION

Protect the confidentiality and integrity of transmitted information.

IMPLEMENTATION DETAILS

Confidential information transmitted over a public network (e.g., the Internet) must be encrypted with, at minimum, a 128-bit encryption algorithm. A SAI may also choose to implement encryption for other data classifications.

SC-12 | CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

CONTROL DESCRIPTION

Establish and manage cryptographic keys when cryptography is employed within the system by the following key management requirements: [organisation-defined requirements for key generation, distribution, storage, access, and destruction].

IMPLEMENTATION DETAILS

Reference the control description above.

SC-13 | CRYPTOGRAPHIC PROTECTION

CONTROL DESCRIPTION

1. Determine the [organisation-defined cryptographic uses]; and

2. Implement the following types of cryptography required for each specified cryptographic use: [organisation-defined types of cryptography for each specified cryptographic use].

IMPLEMENTATION DETAILS

Encryption requirements for information storage devices, data transmissions, and specific requirements for portable devices, removable media, and encryption key standards and management shall be based on documented SAI risk management decisions.

Confidential information transmitted over a public network (e.g., the Internet) must be encrypted as described by SC-8.

Confidential information stored in a public location that is directly accessible without compensating controls (e.g., FTP without access control) must be encrypted.

Storing confidential information on portable devices is discouraged. Confidential information must be encrypted if copied or stored on a portable computing device, removable media, or a non-SAI-owned computing device.

The minimum algorithm strength for protecting confidential information is a 128-bit encryption algorithm, subject to SAI risk management decisions justified and documented.

An organisation may also implement additional protections for other data classifications, including encryption.

SC-15 | COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS

CONTROL DESCRIPTION

1. Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [organisation-defined exceptions where remote activation is to be allowed]; and

2. Provide an explicit indication of use to users physically present at the devices.

IMPLEMENTATION DETAILS

Reference the control description above.

SC-20 | SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

CONTROL DESCRIPTION

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

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.

IMPLEMENTATION DETAILS

Reference the control description above.

SC-21 | SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

CONTROL DESCRIPTION

Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.

IMPLEMENTATION DETAILS

Reference the control description above.

SC-22 | ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE

CONTROL DESCRIPTION

Ensure the systems that collectively provide an organisation's name/address resolution service are fault-tolerant and implement internal and external role separation.

IMPLEMENTATION DETAILS

Reference the control description above.

SC-39 | PROCESS ISOLATION

CONTROL DESCRIPTION

Maintain a separate execution domain for each executing system process.

IMPLEMENTATION DETAILS

Reference the control description above.

SI – SYSTEM AND INFORMATION INTEGRITY

SI-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to [organisation-defined personnel or roles]:

    i. [Select (one or more): organisation-level; mission/business process-level; system-level] system and information integrity policy that:

        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and

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

    ii. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls.

2. Designate an [organisation-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and

3. Review and update the current system and information integrity:

    i. Policy [organisation-defined frequency]; and
    ii. Procedures [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

SI-2 | FLAW REMEDIATION

CONTROL DESCRIPTION

1. Identify, report, and correct system flaws;

2. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

3. Install security-relevant software and firmware updates within [organisation-defined time-period] of the release of the updates; and

4. Incorporate flaw remediation into the organisational configuration management process.

IMPLEMENTATION DETAILS

The SAI identifies, reports, and corrects information system flaws.

SI-3 | MALICIOUS CODE PROTECTION

CONTROL DESCRIPTION

1. Implement [Select (one or more): signature-based; non-signature-based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.

2. Automatically update malicious code protection mechanisms as organisational configuration management policy and procedures make new releases available.

3. Configure malicious code protection mechanisms to:

    i. Perform periodic scans of the system [organisation-defined frequency] and real-time scans of files from external sources at [Select (one or more): endpoint; network entry/exit points] as the files are downloaded, opened, or executed by organisational policy; and

    ii. [Select (one or more)]: block malicious code; quarantine malicious code; take [organisation-defined action]; and send an alert to [organisation-defined personnel or roles] in response to malicious code detection.

4. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the system's availability.

IMPLEMENTATION DETAILS

Reference the control description above.

SI-4 | SYSTEM MONITORING

CONTROL DESCRIPTION

1. Monitor the system to detect:

    i. Attacks and indicators of potential attacks by the following monitoring objectives: [organisation-defined monitoring objectives]; and
    ii. Unauthorised local, network, and remote connections.

2. Identify unauthorised use of the system through the following techniques and methods: [organisation-defined techniques and methods].

3. Invoke internal monitoring capabilities or deploy monitoring devices:

    i. Strategically within the system to collect organisation-determined essential information; and
    ii. At ad hoc locations within the system, track specific transactions of interest to the organisation.

4. Protect information obtained from intrusion-monitoring tools from unauthorised access, modification, and deletion.

5. Adjust the level of system monitoring activity when there is a change in risk to organisational operations and assets, individuals or other organisations;

6. Obtain legal opinion regarding system monitoring activities; and

7. Provide [organisation-defined system monitoring information] to [organisation-defined personnel or roles] [Select (one or more) as needed; [organisation-defined frequency]].

IMPLEMENTATION DETAILS

Each SAI head or their designated representative and information security officer shall establish a security strategy that includes perimeter protection.

The department will provide security information management services, including external network monitoring, scanning, and alerting for SAIs utilising information resources. Perimeter security controls may include some or all components: Demilitarised Zone (DMZ), firewall, intrusion detection or prevention system, or router.

SI-5 | SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

CONTROL DESCRIPTION

1. Continuously receive system security alerts, advisories, and directives from [organisation-defined external organisations].

2. Generate internal security alerts, advisories, and directives as deemed necessary.

3. Disseminate security alerts, advisories, and directives to: [Select (one or more)]: [organisation-defined personnel or roles]; [organisation-defined elements within the organisation]; [organisation-defined external organisations]; and

4. Implement security directives by established time frames or notify the issuing organisation of the degree of noncompliance.

IMPLEMENTATION DETAILS

Reference the control description above.

SI-10 | INFORMATION INPUT VALIDATION

CONTROL DESCRIPTION

Check the validity of the following information inputs: [organisation-defined information inputs to the system].

IMPLEMENTATION DETAILS

Reference the control description above.

SI-12 | INFORMATION MANAGEMENT AND RETENTION

CONTROL DESCRIPTION

Manage and retain information within the system and information output from the system by applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.

IMPLEMENTATION DETAILS

Reference the control description above.

SR – SUPPLY CHAIN RISK MANAGEMENT

SR-1 | POLICY AND PROCEDURES

CONTROL DESCRIPTION

1. Develop, document, and disseminate to [organisation-defined personnel or roles]:

    i. Select (one or more): [organisation-level; mission/business process-level; system-level] or supply chain risk management policy that:

        - Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organisational entities, and compliance; and

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

    ii. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls.

2. Designate an [organisation-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and

3. Review and update the current supply chain risk management:

    i. Policy [organisation-defined frequency]; and
    ii. Procedures [organisation-defined frequency].

IMPLEMENTATION DETAILS

Reference the control description above.

SR-2 | SUPPLY CHAIN RISK MANAGEMENT PLAN

CONTROL DESCRIPTION

1. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, and disposal of the following systems, system components or system services: [organisation-defined systems, system components, or system services].

2. Implement the supply chain risk management plan consistently across the organisation; and

3. Review and update the supply chain risk management plan [organisation-defined frequency] or as required to address threat, organisational or environmental changes.

IMPLEMENTATION DETAILS

Reference the control description above.

SR-3 | SUPPLY CHAIN CONTROLS AND PROCESSES

CONTROL DESCRIPTION

1. Establish processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [organisation-defined system or system component] in coordination with [organisation-defined supply chain personnel].

2. Employ the following supply chain 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: [organisation-defined supply chain controls]; and

3. Document the selected and implemented supply chain processes and controls in [Select: security and privacy plans; supply chain risk management plan; [organisation- defined document]].

IMPLEMENTATION DETAILS

Reference the control description above.

SR-5 | ACQUISITION STRATEGIES, TOOLS, AND METHODS

CONTROL DESCRIPTION

Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [organisation-defined acquisition strategies, contract tools, and procurement methods].

IMPLEMENTATION DETAILS

Reference the control description above.

SR-8 | NOTIFICATION AGREEMENTS

CONTROL DESCRIPTION

Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Select (one or more)]: notification of supply chain compromises; results of assessments or audits; [organisation-defined information].

IMPLEMENTATION DETAILS

Reference the control description above.

SR-12 | COMPONENT DISPOSAL

CONTROL DESCRIPTION

1. Enforce a limit of [organisation-defined number] consecutive invalid logon attempts by a user during a [organisation-defined time-period]; and

2. Automatically [Select (one or more)]: lock the account or node for an [organisation-defined time-period]; lock the account or node until released by an administrator; delay next login prompt per [organisation-defined delay algorithm]; notify system administrator; take other [organisation-defined action] when the maximum number of unsuccessful attempts is exceeded.

IMPLEMENTATION DETAILS

Reference the control description above.