NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document : Secure Controls Framework (SCF) version 2025.3
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: Saudi Arabia IoT CGIoT-1:2024
Focal Document URL: https://cdn.nca.gov.sa/api/files/public/upload/207a41a9-febf-45ea-9517-5519e863028a_CGIoT-.pdf
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-emea-sa-cybersecurity-guidelines-iot.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
1-1	Cybersecurity	To ensure that an organization's overall cybersecurity strategy, vision, plans, goals, initiatives and projects include IoT cybersecurity aspects, and contribute to compliance with relevant laws and regulations.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
1-1-1	N/A	Define, document, and approve IoT cybersecurity requirements within the organization's overall cybersecurity strategy.	Functional	subset of	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	10	
1-1-2	N/A	Develop, document and implement an IoT cybersecurity plan (within the organizational overall cybersecurity plan) outlining the prioritized actions and initiatives to address the cybersecurity risks identified in relation to IoT within the organization.	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
1-1-2	N/A	Develop, document and implement an IoT cybersecurity plan (within the organizational overall cybersecurity plan) outlining the prioritized actions and initiatives to address the cybersecurity risks identified in relation to IoT within the organization.	Functional	subset of	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	10	
1-1-2	N/A	Develop, document and implement an IoT cybersecurity plan (within the organizational overall cybersecurity plan) outlining the prioritized actions and initiatives to address the cybersecurity risks identified in relation to IoT within the organization.	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
1-1-2	N/A	Develop, document and implement an IoT cybersecurity plan (within the organizational overall cybersecurity plan) outlining the prioritized actions and initiatives to address the cybersecurity risks identified in relation to IoT within the organization.	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
1-1-3	N/A	Define and track IoT cybersecurity Key Performance Indicators (KPIs) to ensure fulfilment of the cybersecurity requirements throughout the lifecycle of IoT devices.	Functional	intersects with	Key Performance Indicators (KPIs)	GOV-05.1	Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring and trend analysis of the cybersecurity and data protection program.	5	
1-1-4	N/A	Periodically review at planned intervals and if necessary, update the strategic initiatives and goals, or upon changes in laws and regulations related to IoT cybersecurity as part of the organization cybersecurity steering committee duties.	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
1-1-4	N/A	Periodically review at planned intervals and if necessary, update the strategic initiatives and goals, or upon changes in laws and regulations related to IoT cybersecurity as part of the organization cybersecurity steering committee duties.	Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	3	
1-1-4	N/A	Periodically review at planned intervals and if necessary, update the strategic initiatives and goals, or upon changes in laws and regulations related to IoT cybersecurity as part of the organization cybersecurity steering committee duties.	Functional	intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
1-2	Cybersecurity Policies and Procedures	To ensure that IoT cybersecurity policies and procedures are documented, communicated and complied with by internal stakeholders in the organization, as well as related third parties, as per related laws and regulations, and organizational requirements.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
1-2-1	N/A	Define, document, approve and disseminate policies and procedures for the IoT cybersecurity, as part of the organization's overall cybersecurity policies and procedures with the relevant parties inside and outside the organization, including supply chain partners and third-party service providers.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	
1-2-1	N/A	Define, document, approve and disseminate policies and procedures for the IoT cybersecurity, as part of the organization's overall cybersecurity policies and procedures with the relevant parties inside and outside the organization, including supply chain partners and third-party service providers.	Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
1-2-2	N/A	Support policies and procedures by technical security standards including but not limited to (hardening / minimum baseline security standards for embedded systems, authentication and authorization standards, digital certificates, network zoning security standards, etc).	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
1-2-3	N/A	Periodically review at planned intervals and if necessary, update the policies, procedures and standards as per organizational requirements, or upon changes to related laws and regulations.	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
1-2-3	N/A	Periodically review at planned intervals and if necessary, update the policies, procedures and standards as per organizational requirements, or upon changes to related laws and regulations.	Functional	intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
1-3	Cybersecurity Roles and Responsibilities	To ensure that roles and responsibilities are defined for all the parties, involved in managing, implementing and monitoring IoT cybersecurity requirements within the organization.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
1-3-1	N/A	Define, document and approve IoT cybersecurity roles and responsibilities within the organization's cybersecurity governance structure and roles and responsibilities so that cybersecurity requirements are being addressed in accordance with the organization's policies and procedures.	Functional	equal	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
1-3-2	N/A	Periodically review at planned intervals and if necessary, update the IoT cybersecurity roles and responsibilities as per organizational requirements, or upon changes to related laws and regulations.	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
1-3-2	N/A	Periodically review at planned intervals and if necessary, update the IoT cybersecurity roles and responsibilities as per organizational requirements, or upon changes to related laws and regulations.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	3	
1-4	Cybersecurity Risk Management	To ensure IoT cybersecurity risks are managed using a methodological approach in order to protect the organization's IoT assets as per related laws and regulations, and organizational policies and procedures.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
1-4-1	N/A	Define, document, approve, and implement IoT cybersecurity risk management practices, and identify, assess, respond and oversight IoT cybersecurity risks, in order to minimize the impact of potential threats and attacks on the IoT environment, as part of the organization's cybersecurity risk management methodologies and programs.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
1-4-1	N/A	Define, document, approve, and implement IoT cybersecurity risk management practices, and identify, assess, respond and oversight IoT cybersecurity risks, in order to minimize the impact of potential threats and attacks on the IoT environment, as part of the organization's cybersecurity risk management methodologies and programs.	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
1-4-1	N/A	Define, document, approve, and implement IoT cybersecurity risk management practices, and identify, assess, respond and oversight IoT cybersecurity risks, in order to minimize the impact of potential threats and attacks on the IoT environment, as part of the organization's cybersecurity risk management methodologies and programs.	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
1-4-1	N/A	Define, document, approve, and implement IoT cybersecurity risk management practices, and identify, assess, respond and oversight IoT cybersecurity risks, in order to minimize the impact of potential threats and attacks on the IoT environment, as part of the organization's cybersecurity risk management methodologies and programs.	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
1-4-2	N/A	Define a list of common cybersecurity risk scenarios that could potentially impact the IoT devices and services, related ecosystem or the organization.	Functional	intersects with	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	5	
1-4-3	N/A	Define and document IoT cybersecurity risks in the IoT cybersecurity risk register within the organization's overall cybersecurity risk register.	Functional	intersects with	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
1-4-4	N/A	Conduct an IoT cybersecurity risk assessment considering potential IoT threats, potential scenarios for common IoT attacks, and potential for process disruption and associated damage.	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
1-4-4	N/A	Conduct an IoT cybersecurity risk assessment considering potential IoT threats, potential scenarios for common IoT attacks, and potential for process disruption and associated damage.	Functional	intersects with	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	5	
1-4-4	N/A	Conduct an IoT cybersecurity risk assessment considering potential IoT threats, potential scenarios for common IoT attacks, and potential for process disruption and associated damage.	Functional	intersects with	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5	
1-4-4	N/A	Conduct an IoT cybersecurity risk assessment considering potential IoT threats, potential scenarios for common IoT attacks, and potential for process disruption and associated damage.	Functional	intersects with	Threat Analysis	THR-10	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
1-4-5	N/A	Determine the cybersecurity risks that exceed the risk appetite defined for the IoT and identify suitable risk mitigation measures to lower that risk to, or below, the level of the organization risk appetite.	Functional	intersects with	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	5	
1-4-5	N/A	Determine the cybersecurity risks that exceed the risk appetite defined for the IoT and identify suitable risk mitigation measures to lower that risk to, or below, the level of the organization risk appetite.	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
1-4-5	N/A	Determine the cybersecurity risks that exceed the risk appetite defined for the IoT and identify suitable risk mitigation measures to lower that risk to, or below, the level of the organization risk appetite.	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
1-4-6	N/A	Periodically review at planned intervals and if necessary, update the IoT cybersecurity risk management procedures and practices as per organizational policies and procedures, or upon changes to related laws and regulations, as well as ensuring they're in alignment with the IoT cybersecurity requirements of the organization.	Functional	intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
1-5	Cybersecurity in Information and Technology Project Management	To ensure that IoT cybersecurity requirements are included in project management methodology and procedures in order to protect the confidentiality, integrity and availability of the IoT assets and its components as per organization policies and procedures, and related laws and regulations.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
1-5-1	N/A	Implement leading practices related to 'Secure-by-Design' principles throughout the development lifecycle phases of IoT devices and services.	Functional	subset of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
1-5-2	N/A	Review the IoT devices and services to ensure that cybersecurity requirements are taken into consideration during planning & design phases of the information and technology projects.	Functional	subset of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.	10	
1-5-2	N/A	Review the IoT devices and services to ensure that cybersecurity requirements are taken into consideration during planning & design phases of the information and technology projects.	Functional	subset of	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	10	
1-5-3	N/A	Define a change management procedure for IoT to ensure control over the IoT cybersecurity posture of the organization, including: • Considering change management activities throughout the entire IoT systems, devices and services lifecycle phases, including development and integration phase, maintenance or disposa phase, as well as during updates, patches or functionality changes. • Monitoring and communicating changes to the relevant parties within the organization.	Functional	subset of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
1-5-3	N/A	Define a change management procedure for IoT to ensure control over the IoT cybersecurity posture of the organization, including: • Considering change management activities throughout the entire IoT systems, devices and services lifecycle phases, including development and integration phase, maintenance or disposa phase, as well as during updates, patches or functionality changes. • Monitoring and communicating changes to the relevant parties within the organization.	Functional	intersects with	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5	
1-5-3	N/A	Define a change management procedure for IoT to ensure control over the IoT cybersecurity posture of the organization, including: • Considering change management activities throughout the entire IoT systems, devices and services lifecycle phases, including development and integration phase, maintenance or disposa phase, as well as during updates, patches or functionality changes. • Monitoring and communicating changes to the relevant parties within the organization.	Functional	intersects with	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5	
1-6	Compliance with Cybersecurity Standards, Laws and Regulations	To ensure that the organization's IoT cybersecurity programs and initiatives are compliant with related standards, laws and regulations.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
1-6-1	N/A	Implement adequate enforcement and compliance mechanisms to ensure that organizational IoT requirements, programs, initiatives and activities are compliant with related IoT cybersecurity laws and regulations.	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
1-6-1	N/A	Implement adequate enforcement and compliance mechanisms to ensure that organizational IoT requirements, programs, initiatives and activities are compliant with related IoT cybersecurity laws and regulations.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each system, application and/or service under their control.	5	
1-6-1	N/A	Implement adequate enforcement and compliance mechanisms to ensure that organizational IoT requirements, programs, initiatives and activities are compliant with related IoT cybersecurity laws and regulations.	Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity and data protection controls for each system, application and/or service under their control.	3	
1-6-1	N/A	Implement adequate enforcement and compliance mechanisms to ensure that organizational IoT requirements, programs, initiatives and activities are compliant with related IoT cybersecurity laws and regulations.	Functional	intersects with	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required cybersecurity and data protection controls for each system, application and/or service under their control.	3	
1-6-1	N/A	Implement adequate enforcement and compliance mechanisms to ensure that organizational IoT requirements, programs, initiatives and activities are compliant with related IoT cybersecurity laws and regulations.	Functional	intersects with	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required cybersecurity and data protection controls for each system, application and/or service under their control are implemented correctly and are operating as intended.	3	
1-6-1	N/A	Implement adequate enforcement and compliance mechanisms to ensure that organizational IoT requirements, programs, initiatives and activities are compliant with related IoT cybersecurity laws and regulations.	Functional	intersects with	Authorize Systems, Applications & Services	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each system, application and/or service under their control.	3	
1-6-1	N/A	Implement adequate enforcement and compliance mechanisms to ensure that organizational IoT requirements, programs, initiatives and activities are compliant with related IoT cybersecurity laws and regulations.	Functional	intersects with	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor Technology Assets, Applications and/or Services (TAAS) under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity and data protection controls are operating as intended.	3	
1-7	Periodical Cybersecurity Review and Audit	To ensure that organizational IoT cybersecurity requirements are implemented and in compliance with the organizational policies and procedures, as well as related national laws and regulations, and any other related regulations.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
1-7-1	N/A	Review the implementation of IoT cybersecurity requirements, within the organization, periodically by the cybersecurity function.	Functional	intersects with	Periodic Audits	CPL-02.2	Mechanisms exist to conduct periodic audits of cybersecurity and data protection controls to evaluate conformity with the organization's documented policies, standards and procedures.	5	
1-7-1	N/A	Review the implementation of IoT cybersecurity requirements, within the organization, periodically by the cybersecurity function.	Functional	subset of	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity and data protection policies and standards.	10	
1-7-2	N/A	Review and audit periodically by independent parties outside the cybersecurity function or by third party as part of the overall review and audit of cybersecurity requirements in the organization to ensure implementation and compliance with IoT cybersecurity requirements, and document the results.	Functional	intersects with	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate cybersecurity and data protection controls at planned intervals or when the system, service or project undergoes significant changes.	8	
1-7-3	N/A	Define and implement a process to record and manage any non-compliance with IoT cybersecurity requirements, in addition to assigning roles and responsibilities to implement recommendations and corrective actions to address the identified non-compliance cases, and ensure that summary results and recommendations are made available to accountable individuals within the organization and the cybersecurity steering committee.	Functional	subset of	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	10	
1-7-3	N/A	Define and implement a process to record and manage any non-compliance with IoT cybersecurity requirements, in addition to assigning roles and responsibilities to implement recommendations and corrective actions to address the identified non-compliance cases, and ensure that summary results and recommendations are made available to accountable individuals within the organization and the cybersecurity steering committee.	Functional	intersects with	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	5	
1-8	Cybersecurity in Human Resources	To ensure that IoT cybersecurity risks related to personnel (employees and contractors) in organizations are managed effectively during the employment lifecycle as per organizational policies and procedures, and related laws and regulations.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
1-8-1	N/A	Define, document, approve, and implement IoT cybersecurity requirements for personnel in organizations (prior to employment, during employment and after termination/separation). This may include: • Cybersecurity induction and ongoing training requirements for personnel, with a specific focus on IoT cybersecurity requirements. • Implementation of and compliance with the IoT cybersecurity requirements.	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
1-8-1	N/A	Define, document, approve, and implement IoT cybersecurity requirements for personnel in organizations (prior to employment, during employment and after termination/separation). This may include: • Cybersecurity induction and ongoing training requirements for personnel, with a specific focus on IoT cybersecurity requirements. • Implementation of and compliance with the IoT cybersecurity requirements.	Functional	intersects with	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	5	
1-8-1	N/A	Define, document, approve, and implement IoT cybersecurity requirements for personnel in organizations (prior to employment, during employment and after termination/separation). This may include: • Cybersecurity induction and ongoing training requirements for personnel, with a specific focus on IoT cybersecurity requirements. • Implementation of and compliance with the IoT cybersecurity requirements.	Functional	intersects with	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
1-8-1	N/A	Define, document, approve, and implement IoT cybersecurity requirements for personnel in organizations (prior to employment, during employment and after termination/separation). This may include: • Cybersecurity induction and ongoing training requirements for personnel, with a specific focus on IoT cybersecurity requirements. • Implementation of and compliance with the IoT cybersecurity requirements.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
1-8-2	N/A	Periodically review personnel access to IoT devices and services, and update or revoke access permissions immediately upon changing roles or termination/separation.	Functional	intersects with	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	5	
1-8-2	N/A	Periodically review personnel access to IoT devices and services, and update or revoke access permissions immediately upon changing roles or termination/separation.	Functional	intersects with	System Account Reviews	IAC-15.7	Mechanisms exist to review all system accounts and disable any account that cannot be associated with a business process and owner.	5	
1-8-2	N/A	Periodically review personnel access to IoT devices and services, and update or revoke access permissions immediately upon changing roles or termination/separation.	Functional	intersects with	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	
1-8-3	N/A	Periodically review at planned intervals and if necessary, update the IoT cybersecurity requirements for personnel in organizations as per organizational policies and procedures or upon changes to related laws and regulations.	Functional	intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
1-9	Cybersecurity Awareness and Training Program	To ensure that personnel have essential IoT cybersecurity awareness, and are provided with specific IoT cybersecurity training, skills and credentials needed to accomplish their cybersecurity responsibilities of protecting the organization's IoT assets.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
1-9-1	N/A	Include IoT cybersecurity aspects within the organization's overall cybersecurity awareness and training strategy, including: • Define, document, and approve training strategy for personnel with specific IoT roles and responsibilities. • Train employees on cybersecurity best practices for the secure usage of IoT devices and services. • Embed training programs with information about IoT cybersecurity best practices, roles and responsibilities, policies and standards to ensure a safe work environment.	Functional	subset of	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
1-9-1	N/A	Include IoT cybersecurity aspects within the organization's overall cybersecurity awareness and training strategy, including: • Define, document, and approve training strategy for personnel with specific IoT roles and responsibilities. • Train employees on cybersecurity best practices for the secure usage of IoT devices and services. • Embed training programs with information about IoT cybersecurity best practices, roles and responsibilities, policies and standards to ensure a safe work environment.	Functional	intersects with	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
1-9-1	N/A	Include IoT cybersecurity aspects within the organization's overall cybersecurity awareness and training strategy, including: • Define, document, and approve training strategy for personnel with specific IoT roles and responsibilities. • Train employees on cybersecurity best practices for the secure usage of IoT devices and services. • Embed training programs with information about IoT cybersecurity best practices, roles and responsibilities, policies and standards to ensure a safe work environment.	Functional	intersects with	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
1-9-2	N/A	Promote IoT cybersecurity awareness at all organization levels, considering the following; • Keeping personnel aware at all organization levels of the importance of safeguarding IoT devices, including decision-makers. • Conducting cybersecurity activities to raise IoT cybersecurity awareness among personnel, through courses, IoT cybersecurity simulations activties, cybersecurity best practices brochures via e-mail, round tables, and any other awareness channel. • Assessing the IoT cybersecurity skills of personnel to identify knowledge gaps, and efficiently map training against the required skills for each job. • Ensuring that personnel working with IoT devices and services are updated with the latest developments of in the field of IoT cybersecurity.	Functional	intersects with	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
1-9-2	N/A	Promote IoT cybersecurity awareness at all organization levels, considering the following; • Keeping personnel aware at all organization levels of the importance of safeguarding IoT devices, including decision-makers. • Conducting cybersecurity activities to raise IoT cybersecurity awareness among personnel, through courses, IoT cybersecurity simulations activties, cybersecurity best practices brochures via e-mail, round tables, and any other awareness channel. • Assessing the IoT cybersecurity skills of personnel to identify knowledge gaps, and efficiently map training against the required skills for each job. • Ensuring that personnel working with IoT devices and services are updated with the latest developments of in the field of IoT cybersecurity.	Functional	intersects with	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity and data protection awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
2-1	Asset Management	To ensure that the organization has an accurate and detailed inventory of IoT assets in order to maintain their confidentiality, integrity and availability, in alignment with the organization's cybersecurity and operational requirements.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
2-1-1	N/A	Maintain an inventory of the different types of IoT devices and services related assets used by the organization, including naming, classification, sensitivity, components, hardware and software capabilities, as well as those of third parties, as the capabilities of IoT devices vary with their different types, which may expose the oragnization's IoT environment to various risks.	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
2-1-2	N/A	Review periodically the IoT inventory, and track all changes within the organization.	Functional	intersects with	Updates During Installations / Removals	AST-02.1	Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.	5	
2-1-2	N/A	Review periodically the IoT inventory, and track all changes within the organization.	Functional	intersects with	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
2-2	Identity and Access Management	To prevent unauthorized access to IoT assets and restrict access to what is that is necessary to accomplish tasks for the organization.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
2-2-1	N/A	Manage access identities and permissions to IoT assets and restrict access to IoT data, services and devices to authorized users only, based on access and permission control principles (need-to- know-and-use, least privileges, and segregation of duties). In addition to managing privileged access accounts on IoT devices and services.	Functional	intersects with	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	
2-2-1	N/A	Manage access identities and permissions to IoT assets and restrict access to IoT data, services and devices to authorized users only, based on access and permission control principles (need-to- know-and-use, least privileges, and segregation of duties). In addition to managing privileged access accounts on IoT devices and services.	Functional	intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
2-2-1	N/A	Manage access identities and permissions to IoT assets and restrict access to IoT data, services and devices to authorized users only, based on access and permission control principles (need-to- know-and-use, least privileges, and segregation of duties). In addition to managing privileged access accounts on IoT devices and services.	Functional	intersects with	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	5	
2-2-1	N/A	Manage access identities and permissions to IoT assets and restrict access to IoT data, services and devices to authorized users only, based on access and permission control principles (need-to- know-and-use, least privileges, and segregation of duties). In addition to managing privileged access accounts on IoT devices and services.	Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
2-2-2	N/A	Implement strong authentication standard to access IoT devices and services, and follow best practices, including but not limited to: • Prevent the users from using default and hard-coded passwords. • Enforce the users to change their passwords periodically. • Improve the complexity of passwords, such as by defining a minimum key length and usage of a combination ofletters (upper/lower cases), numbers and symbols; • Implement controls to prevent the display of user's credentials on login interfaces in applications. • Establish threshold limits for unsuccessful attempts. • Enable secure authentication capabilities, if applicable.	Functional	intersects with	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
2-2-2	N/A	Implement strong authentication standard to access IoT devices and services, and follow best practices, including but not limited to: • Prevent the users from using default and hard-coded passwords. • Enforce the users to change their passwords periodically. • Improve the complexity of passwords, such as by defining a minimum key length and usage of a combination ofletters (upper/lower cases), numbers and symbols; • Implement controls to prevent the display of user's credentials on login interfaces in applications. • Establish threshold limits for unsuccessful attempts. • Enable secure authentication capabilities, if applicable.	Functional	intersects with	Password-Based Authentication	IAC-10.1	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	5	
2-2-2	N/A	Implement strong authentication standard to access IoT devices and services, and follow best practices, including but not limited to: • Prevent the users from using default and hard-coded passwords. • Enforce the users to change their passwords periodically. • Improve the complexity of passwords, such as by defining a minimum key length and usage of a combination ofletters (upper/lower cases), numbers and symbols; • Implement controls to prevent the display of user's credentials on login interfaces in applications. • Establish threshold limits for unsuccessful attempts. • Enable secure authentication capabilities, if applicable.	Functional	intersects with	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5	
2-2-2	N/A	Implement strong authentication standard to access IoT devices and services, and follow best practices, including but not limited to: • Prevent the users from using default and hard-coded passwords. • Enforce the users to change their passwords periodically. • Improve the complexity of passwords, such as by defining a minimum key length and usage of a combination ofletters (upper/lower cases), numbers and symbols; • Implement controls to prevent the display of user's credentials on login interfaces in applications. • Establish threshold limits for unsuccessful attempts. • Enable secure authentication capabilities, if applicable.	Functional	intersects with	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	5	
2-2-3	N/A	Review periodically the IoT access identities and permissions, based on access and permission control principles.	Functional	intersects with	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	
2-3	Email and Messaging Services Protection	To ensure the implementation of cybersecurity requirements for protecting communicating IoT data over email and other messaging services such as SMS, to protect this data from cybersecurity risks.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
2-3-1	N/A	Define, document, and approve cybersecurity requirements for protecting the data transmitted between the IoT devices/services and the organization's email and messaging services and review periodically.	Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
2-3-1	N/A	Define, document, and approve cybersecurity requirements for protecting the data transmitted between the IoT devices/services and the organization's email and messaging services and review periodically.	Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
2-3-2	N/A	Implement cybersecurity requirements for protecting the data transmitted between the IoT devices/services and the organization's email and messaging services, as part of the organization's email and messaging services protection measures.	Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
2-3-2	N/A	Implement cybersecurity requirements for protecting the data transmitted between the IoT devices/services and the organization's email and messaging services, as part of the organization's email and messaging services protection measures.	Functional	intersects with	Electronic Messaging	NET-13	Mechanisms exist to protect the confidentiality, integrity and availability of electronic messaging communications.	5	
2-4	Network Security Management	To develop secure and reliable communication and integration capabilities between different IoT devices operating in a network.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
2-4-1	N/A	Define, document, approve, and implement cybersecurity requirements for secure connectivity between the IoT devices/services and the intended usage environment including other devices and technology/cloud infrastructure and review periodically.	Functional	intersects with	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
2-4-1	N/A	Define, document, approve, and implement cybersecurity requirements for secure connectivity between the IoT devices/services and the intended usage environment including other devices and technology/cloud infrastructure and review periodically.	Functional	intersects with	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
2-4-1	N/A	Define, document, approve, and implement cybersecurity requirements for secure connectivity between the IoT devices/services and the intended usage environment including other devices and technology/cloud infrastructure and review periodically.	Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
2-4-2	N/A	Implement measures to secure the data communication between different devices connected in a network, including authentication of the peer device with which an IoT device is trying to communicate.	Functional	intersects with	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
2-4-2	N/A	Implement measures to secure the data communication between different devices connected in a network, including authentication of the peer device with which an IoT device is trying to communicate.	Functional	intersects with	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
2-4-3	N/A	Encrypt and authenticate data transactions between different IoT devices and services, as well as secure the underlying infrastructure, where applicable.	Functional	intersects with	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
2-4-3	N/A	Encrypt and authenticate data transactions between different IoT devices and services, as well as secure the underlying infrastructure, where applicable.	Functional	intersects with	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
2-4-4	N/A	Implement logical and/or physical segregations between IoT environment and organization's environment based on the organization's cybersecurity risk assessment, where applicable.	Functional	intersects with	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
2-4-5	N/A	Deploy security gateways to internet-facing IoT devices and services to secure all communication and connectivity to the internet.	Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
2-4-5	N/A	Deploy security gateways to internet-facing IoT devices and services to secure all communication and connectivity to the internet.	Functional	intersects with	Boundary Protection	NET-03	Mechanisms exist to monitor and control communications at the external network boundary and at key internal boundaries within the network.	5	
2-4-6	N/A	Use secure update servers to ensure that the update file for the IoT device software/ firmware, its configuration, and its applications, is transmitted over a secure connection and ensure adequate authentication and encryption mechanisms are put in place to transmit the updates.	Functional	subset of	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	10	
2-4-6	N/A	Use secure update servers to ensure that the update file for the IoT device software/ firmware, its configuration, and its applications, is transmitted over a secure connection and ensure adequate authentication and encryption mechanisms are put in place to transmit the updates.	Functional	intersects with	Embedded Technology Maintenance	EMB-07	Mechanisms exist to securely update software and upgrade functionality on embedded devices.	5	
2-4-6	N/A	Use secure update servers to ensure that the update file for the IoT device software/ firmware, its configuration, and its applications, is transmitted over a secure connection and ensure adequate authentication and encryption mechanisms are put in place to transmit the updates.	Functional	intersects with	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
2-5	IoT-Connected Mobile Devices Security	To ensure the implementation of cybersecurity requirements for mobile devices (including but not limited to smartphones and smart tablets devices) that are connected to IoT devices and services, to enhance security and reduce the cyber risks.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
2-5-1	N/A	Implement the following measures for IoT-connected mobile devices : • Implement measures to secure the communication between the IoT device and the mobile devices. • Restrict the access to IoT-connected mobile devices only to authorized personnel. • Use secure methods of authentication for accessing the mobile device and IoT device data. • Implement secure code development practices for mobile applications interacting with the IoT devices. • Secure erasure of IoT devices stored data when losing the mobile device, or when the device is no longer used.	Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
2-5-1	N/A	Implement the following measures for IoT-connected mobile devices : • Implement measures to secure the communication between the IoT device and the mobile devices. • Restrict the access to IoT-connected mobile devices only to authorized personnel. • Use secure methods of authentication for accessing the mobile device and IoT device data. • Implement secure code development practices for mobile applications interacting with the IoT devices. • Secure erasure of IoT devices stored data when losing the mobile device, or when the device is no longer used.	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
2-5-1	N/A	Implement the following measures for IoT-connected mobile devices : • Implement measures to secure the communication between the IoT device and the mobile devices. • Restrict the access to IoT-connected mobile devices only to authorized personnel. • Use secure methods of authentication for accessing the mobile device and IoT device data. • Implement secure code development practices for mobile applications interacting with the IoT devices. • Secure erasure of IoT devices stored data when losing the mobile device, or when the device is no longer used.	Functional	subset of	Embedded Technology Security Program	EMB-01	Mechanisms exist to facilitate the implementation of embedded technology controls.	10	
2-5-1	N/A	Implement the following measures for IoT-connected mobile devices : • Implement measures to secure the communication between the IoT device and the mobile devices. • Restrict the access to IoT-connected mobile devices only to authorized personnel. • Use secure methods of authentication for accessing the mobile device and IoT device data. • Implement secure code development practices for mobile applications interacting with the IoT devices. • Secure erasure of IoT devices stored data when losing the mobile device, or when the device is no longer used.	Functional	intersects with	Internet of Things (IOT)	EMB-02	Mechanisms exist to proactively manage the cybersecurity and data protection risks associated with Internet of Things (IoT).	5	
2-5-1	N/A	Implement the following measures for IoT-connected mobile devices : • Implement measures to secure the communication between the IoT device and the mobile devices. • Restrict the access to IoT-connected mobile devices only to authorized personnel. • Use secure methods of authentication for accessing the mobile device and IoT device data. • Implement secure code development practices for mobile applications interacting with the IoT devices. • Secure erasure of IoT devices stored data when losing the mobile device, or when the device is no longer used.	Functional	subset of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
2-6	Data and Information Protection	To ensure confidentiality, integrity and abilability of data processed by IoT devices and services.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
2-6-1	N/A	Implement IoT data classification and labeling mechanisms for the IoT devices and services as per related laws and regulations, and organizational requirements.	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
2-6-1	N/A	Implement IoT data classification and labeling mechanisms for the IoT devices and services as per related laws and regulations, and organizational requirements.	Functional	intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
2-6-1	N/A	Implement IoT data classification and labeling mechanisms for the IoT devices and services as per related laws and regulations, and organizational requirements.	Functional	intersects with	Component Marking	PES-16	Physical security mechanisms exist to mark system hardware components indicating the impact or classification level of the information permitted to be processed, stored or transmitted by the hardware component.	5	
2-6-2	N/A	Implement prevention measures to avoid unauthorized access to and tamper with IoT data at rest or in transit.	Functional	intersects with	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5	
2-6-2	N/A	Implement prevention measures to avoid unauthorized access to and tamper with IoT data at rest or in transit.	Functional	intersects with	Logical Tampering Protection	AST-15	Mechanisms exist to verify logical configuration settings and the physical integrity of critical technology assets throughout their lifecycle.	5	
2-6-2	N/A	Implement prevention measures to avoid unauthorized access to and tamper with IoT data at rest or in transit.	Functional	intersects with	Prevent Alterations	EMB-06	Mechanisms exist to protect embedded devices by preventing the unauthorized installation and execution of software.	5	
2-6-3	N/A	Prevent IoT devices from collecting sensitive data that is not needed or cannot be adequately protected.	Functional	Subset Of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
2-6-3	N/A	Prevent IoT devices from collecting sensitive data that is not needed or cannot be adequately protected.	Functional	intersects with	Collection Minimization	END-13.3	Mechanisms exist to utilize sensors that are configured to minimize the collection of information about individuals.	3	
2-7	Cryptography	To ensure adequate use of cryptographic capabilities to secure data transactions and exchange between IoT devices.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
2-7-1	N/A	Define, document, approve, and implement cybersecurity requirements for IoT data following the National Cryptographic Standards (NCS-1:2020) and review periodically.	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
2-7-2	N/A	Encrypt the data, both at rest or in transit, where applicable.	Functional	intersects with	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
2-7-2	N/A	Encrypt the data, both at rest or in transit, where applicable.	Functional	intersects with	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
2-8	Backup and Recovery Method	To ensure implementation of backup and recovery capabilities within IoT devices and services, in order to protect the data processed by IoT devices from cyber risks.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
2-8-1	N/A	Define, document, approve and implement IoT cybersecurity requirements for backup and recovery management as part of the organization's overall backup and recovery management policies and review periodically.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
2-8-1	N/A	Define, document, approve and implement IoT cybersecurity requirements for backup and recovery management as part of the organization's overall backup and recovery management policies and review periodically.	Functional	intersects with	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
2-8-2	N/A	Maintain a tested and trusted version of the IoT software and data stored locally, to enable safe recovery.	Functional	intersects with	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
2-8-2	N/A	Maintain a tested and trusted version of the IoT software and data stored locally, to enable safe recovery.	Functional	intersects with	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	5	
2-8-3	N/A	Review periodically the stored backups for the IoT devices and test them.	Functional	intersects with	Test Restoration Using Sampling	BCD-11.5	Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.	5	
2-9	Vulnerability Management	To ensure timely detection and remediation of vulnerabilities, so as to prevent the probability of exploiting the vulnerabilities to launch cyberattacks against the organization.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
2-9-1	N/A	Continuously identify, monitor, and mitigate cybersecurity vulnerabilities within the IoT devices and services.	Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
2-9-1	N/A	Continuously identify, monitor, and mitigate cybersecurity vulnerabilities within the IoT devices and services.	Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
2-9-1	N/A	Continuously identify, monitor, and mitigate cybersecurity vulnerabilities within the IoT devices and services.	Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
2-9-2	N/A	Patch all the software/firmeware components within the IoT devices in a timely manner as following: • Implement software patches in a preventative manner, to ensure cybersecurity vulnerabilities are eliminated before they can be exploited. • Ensure that the essential function of the device is maintained during software patching. • Utilize the most recent operating system for development the IoT device, as it would help ensure that known vulnerabilities have been mitigated.	Functional	subset of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	10	
2-10	Penetration Testing	To assess and evaluate the efficiency of the organization's IoT cybersecurity defense capabilities through simulated cyber-attacks, in order to discover unknown weaknesses that may lead to a cyber breach.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
2-10-1	N/A	Perform penteration testing activties to achieve early detection of vulnerable IoT software and hardware components. The approach can comprise the following: • Identification and analysis of IoT assets within the penteration testing scope. • Verification and exploitation of known vulnerabilities, as well as identification of unknown vulnerabilities (Zero-Day Vulnerabilities) in the IoT devices and services. • Identification and assessment of insecure configurations at the application, network, data, and/ or at the sensor or device gateway level. • Development and Implementation of appropriate reporting and alarming procedures to help prioritize decisions on where and how to incorporate additional cybersecurity measures.	Functional	intersects with	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	8	
2-10-2	N/A	Carry out red team exercises targeting mission critical IoT devices and services to simulate social engineering, physical intrusion, hacking and other deceptive techniques aimed at gaining unauthorized access to critical information and assets, where applicable.	Functional	intersects with	Red Team Exercises	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise Technology Assets, Applications and/or Services (TAAS) in accordance with organization-defined rules of engagement.	5	
2-11	Cybersecurity Event Logs and Monitoring Management	To ensure regular collection, monitoring and analysis of IoT cybersecurity event logs and threat cases, in order to enable early detection of a potential cyberattacks across IoT devices and services.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
2-11-1	N/A	Ensure that IoT devices to have the ability to record cybersecurity events, and centrally store it to be monitored by the Security Operations Center (SOC) in the organization, if possible. Taking into consideration the following: • Define the scenarios to discover potential IoT cybersecurity incidents. • Record events such as user authentication, management of accounts and access rights, attempts to access sensitive data, and modifications to system resources. • Monitor, review and analyze event logs and threat cases for IoT on a regular basis. If possible, implement automated systems to enable real-time monitoring oflogs and threat cases. • Leverage data storage services that store the log data in a remote location, instead of storing locally, so that even if the IoT software and hardware components are compromised the log data would remain secure. Implement authentication mechanisms for accessing the data storage to enable secure retrieval of the log data. • In case an unauthorized change or behavior is observed in the IoT assets, alert the consumer and/ or the administrator while ensuring that the device does not connect to a wider network than is necessary to enable the alerting function. • Analyze potential misuse of access privileges by internal stakeholders; • Examine telemetry data collected by IoT devices and services, such as usage, measurement and log data, for cybersecurity anomalies and identifying unusual circumstances in a timely manner. • Establish a retention period for cybersecurity events data. The retention period should be at least 12 months from the date of recording.	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
2-11-1	N/A	Ensure that IoT devices to have the ability to record cybersecurity events, and centrally store it to be monitored by the Security Operations Center (SOC) in the organization, if possible. Taking into consideration the following: • Define the scenarios to discover potential IoT cybersecurity incidents. • Record events such as user authentication, management of accounts and access rights, attempts to access sensitive data, and modifications to system resources. • Monitor, review and analyze event logs and threat cases for IoT on a regular basis. If possible, implement automated systems to enable real-time monitoring oflogs and threat cases. • Leverage data storage services that store the log data in a remote location, instead of storing locally, so that even if the IoT software and hardware components are compromised the log data would remain secure. Implement authentication mechanisms for accessing the data storage to enable secure retrieval of the log data. • In case an unauthorized change or behavior is observed in the IoT assets, alert the consumer and/ or the administrator while ensuring that the device does not connect to a wider network than is necessary to enable the alerting function. • Analyze potential misuse of access privileges by internal stakeholders; • Examine telemetry data collected by IoT devices and services, such as usage, measurement and log data, for cybersecurity anomalies and identifying unusual circumstances in a timely manner. • Establish a retention period for cybersecurity events data. The retention period should be at least 12 months from the date of recording.	Functional	intersects with	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
2-11-1	N/A	Ensure that IoT devices to have the ability to record cybersecurity events, and centrally store it to be monitored by the Security Operations Center (SOC) in the organization, if possible. Taking into consideration the following: • Define the scenarios to discover potential IoT cybersecurity incidents. • Record events such as user authentication, management of accounts and access rights, attempts to access sensitive data, and modifications to system resources. • Monitor, review and analyze event logs and threat cases for IoT on a regular basis. If possible, implement automated systems to enable real-time monitoring oflogs and threat cases. • Leverage data storage services that store the log data in a remote location, instead of storing locally, so that even if the IoT software and hardware components are compromised the log data would remain secure. Implement authentication mechanisms for accessing the data storage to enable secure retrieval of the log data. • In case an unauthorized change or behavior is observed in the IoT assets, alert the consumer and/ or the administrator while ensuring that the device does not connect to a wider network than is necessary to enable the alerting function. • Analyze potential misuse of access privileges by internal stakeholders; • Examine telemetry data collected by IoT devices and services, such as usage, measurement and log data, for cybersecurity anomalies and identifying unusual circumstances in a timely manner. • Establish a retention period for cybersecurity events data. The retention period should be at least 12 months from the date of recording.	Functional	intersects with	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
2-11-1	N/A	Ensure that IoT devices to have the ability to record cybersecurity events, and centrally store it to be monitored by the Security Operations Center (SOC) in the organization, if possible. Taking into consideration the following: • Define the scenarios to discover potential IoT cybersecurity incidents. • Record events such as user authentication, management of accounts and access rights, attempts to access sensitive data, and modifications to system resources. • Monitor, review and analyze event logs and threat cases for IoT on a regular basis. If possible, implement automated systems to enable real-time monitoring oflogs and threat cases. • Leverage data storage services that store the log data in a remote location, instead of storing locally, so that even if the IoT software and hardware components are compromised the log data would remain secure. Implement authentication mechanisms for accessing the data storage to enable secure retrieval of the log data. • In case an unauthorized change or behavior is observed in the IoT assets, alert the consumer and/ or the administrator while ensuring that the device does not connect to a wider network than is necessary to enable the alerting function. • Analyze potential misuse of access privileges by internal stakeholders; • Examine telemetry data collected by IoT devices and services, such as usage, measurement and log data, for cybersecurity anomalies and identifying unusual circumstances in a timely manner. • Establish a retention period for cybersecurity events data. The retention period should be at least 12 months from the date of recording.	Functional	intersects with	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5	
2-11-2	N/A	Conduct regular examination of diagnostic information for IoT devices, including details such as temperature data, memory usage data, battery life and process execution data to enable better identification of any potential cybersecurity incident.	Functional	intersects with	Embedded Technology Configuration Monitoring	EMB-05	Mechanisms exist to generate log entries on embedded devices when configuration changes or attempts to access interfaces are detected.	5	
2-11-2	N/A	Conduct regular examination of diagnostic information for IoT devices, including details such as temperature data, memory usage data, battery life and process execution data to enable better identification of any potential cybersecurity incident.	Functional	intersects with	Power Level Monitoring	EMB-09	Automated mechanisms exist to monitor the power levels of embedded technologies for decreased or excessive power usage, including battery drainage, to investigate for device tampering.	5	
2-12	Cybersecurity Incident and Threat Management	To ensure timely identification and remediation of threats and IoT cybersecurity incidents in order to minimize the negative impact on the organization's operations.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
2-12-1	N/A	Incorporate an IoT incident and threat management model within the overall cybersecurity incident and threat management activities and programs of the organization.	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	3	
2-12-1	N/A	Incorporate an IoT incident and threat management model within the overall cybersecurity incident and threat management activities and programs of the organization.	Functional	intersects with	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5	
2-12-2	N/A	Establish an IoT cybersecurity incident management plan, comprising incident response and handling procedures in alignment with the organization's overall incident management practices. Which can include the following: • Prepare for incidents by ensuring that systems, networks, and applications are secure. • Detect, analyze and document the incident. • Communicate the incident with the stakeholders including the National Cybersecurity Authority (NCA). • Contain, eradicate and recover from the incident. • Create a follow up report for the incident.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
2-12-2	N/A	Establish an IoT cybersecurity incident management plan, comprising incident response and handling procedures in alignment with the organization's overall incident management practices. Which can include the following: • Prepare for incidents by ensuring that systems, networks, and applications are secure. • Detect, analyze and document the incident. • Communicate the incident with the stakeholders including the National Cybersecurity Authority (NCA). • Contain, eradicate and recover from the incident. • Create a follow up report for the incident.	Functional	intersects with	Information System Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	8	
2-12-2	N/A	Establish an IoT cybersecurity incident management plan, comprising incident response and handling procedures in alignment with the organization's overall incident management practices. Which can include the following: • Prepare for incidents by ensuring that systems, networks, and applications are secure. • Detect, analyze and document the incident. • Communicate the incident with the stakeholders including the National Cybersecurity Authority (NCA). • Contain, eradicate and recover from the incident. • Create a follow up report for the incident.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	8	
2-12-2	N/A	Establish an IoT cybersecurity incident management plan, comprising incident response and handling procedures in alignment with the organization's overall incident management practices. Which can include the following: • Prepare for incidents by ensuring that systems, networks, and applications are secure. • Detect, analyze and document the incident. • Communicate the incident with the stakeholders including the National Cybersecurity Authority (NCA). • Contain, eradicate and recover from the incident. • Create a follow up report for the incident.	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
2-12-2	N/A	Establish an IoT cybersecurity incident management plan, comprising incident response and handling procedures in alignment with the organization's overall incident management practices. Which can include the following: • Prepare for incidents by ensuring that systems, networks, and applications are secure. • Detect, analyze and document the incident. • Communicate the incident with the stakeholders including the National Cybersecurity Authority (NCA). • Contain, eradicate and recover from the incident. • Create a follow up report for the incident.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
2-12-2	N/A	Establish an IoT cybersecurity incident management plan, comprising incident response and handling procedures in alignment with the organization's overall incident management practices. Which can include the following: • Prepare for incidents by ensuring that systems, networks, and applications are secure. • Detect, analyze and document the incident. • Communicate the incident with the stakeholders including the National Cybersecurity Authority (NCA). • Contain, eradicate and recover from the incident. • Create a follow up report for the incident.	Functional	intersects with	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
2-12-3	N/A	Establish a post incident analysis capability to identify and assess the specific software and hardware elements of the IoT devices that were impacted. This analysis should then be utilized to provide the necessary cybersecurity updates or engage in device recall activity (as per applicability) to implement the necessary cybersecurity updates, such as upgrading old firmware with default passwords.	Functional	intersects with	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
2-12-4	N/A	Define IoT cybersecurity requirements for threat management as part of the overall threat modelling process developed by the organization. Implement the following practices as part of the IoT threat management plan: • Monitor, track and aggregate threat intelligence data derived from the usage of IoT devices and services. • Share information regarding breach indicators and threat intelligence with the National Cybersecurity Authority (NCA). • Periodically review the cybersecurity requirements for threat management.	Functional	subset of	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
2-12-4	N/A	Define IoT cybersecurity requirements for threat management as part of the overall threat modelling process developed by the organization. Implement the following practices as part of the IoT threat management plan: • Monitor, track and aggregate threat intelligence data derived from the usage of IoT devices and services. • Share information regarding breach indicators and threat intelligence with the National Cybersecurity Authority (NCA). • Periodically review the cybersecurity requirements for threat management.	Functional	intersects with	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
2-12-4	N/A	Define IoT cybersecurity requirements for threat management as part of the overall threat modelling process developed by the organization. Implement the following practices as part of the IoT threat management plan: • Monitor, track and aggregate threat intelligence data derived from the usage of IoT devices and services. • Share information regarding breach indicators and threat intelligence with the National Cybersecurity Authority (NCA). • Periodically review the cybersecurity requirements for threat management.	Functional	intersects with	Threat Intelligence Reporting	THR-03.1	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.	5	
2-13	Physical Security	To ensure the protection of IoT assets from unauthorized physical access, loss, theft and damage.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
2-13-1	N/A	Implement physical detection systems to monitor the critical physical environment related to IoT devices and services, which could include server rooms or other workplace areas dedicated towards managing an organization's network, external communication, or external services such as cloud, internet and surveillance.	Functional	intersects with	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	
2-13-1	N/A	Implement physical detection systems to monitor the critical physical environment related to IoT devices and services, which could include server rooms or other workplace areas dedicated towards managing an organization's network, external communication, or external services such as cloud, internet and surveillance.	Functional	intersects with	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	5	
2-13-2	N/A	Implement hardware tamper protection and detection measures for the IoT devices.	Functional	intersects with	Physical Tampering Detection	AST-08	Mechanisms exist to periodically inspect systems and system components for Indicators of Compromise (IoC).	5	
2-14	IoT Application Security	To ensure the security and reliability of software applications running on IoT devices.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
2-14-1	N/A	Implement technical cybersecurity measures to secure interfaces of IoT applications, in order to reduce the exposure of data, configuration and management operations and prevent unauthorized access.	Functional	intersects with	Interface Security	EMB-04	Mechanisms exist to protect embedded devices against unauthorized use of the physical factory diagnostic and test interface(s).	5	
2-14-2	N/A	Implement measures to whitelist certain applications that can run on the IoT device operating system to help prevent execution of unauthorized malware and applications, including untrusted third-party applications.	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
2-14-2	N/A	Implement measures to whitelist certain applications that can run on the IoT device operating system to help prevent execution of unauthorized malware and applications, including untrusted third-party applications.	Functional	intersects with	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
2-14-3	N/A	Implement secure code development practices for IoT applications and conduct source code review to reduce cybersecurity bugs.	Functional	intersects with	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
2-14-3	N/A	Implement secure code development practices for IoT applications and conduct source code review to reduce cybersecurity bugs.	Functional	intersects with	Software Design Review	TDA-06.5	Mechanisms exist to have an independent review of the software design to confirm that all cybersecurity and data protection requirements are met and that any identified risks are satisfactorily addressed.	3	
2-14-4	N/A	The whitelisted applications should be periodically updated to include new applications, functionalities and software patches.	Functional	intersects with	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5	
2-15	IoT Device Lifestyle Management	To ensure secure installation and set-up ofIoT devices and presence of device withdrawal and replacement plans.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
2-15-1	N/A	Utilize hardware that embeds cybersecurity functions at the component level, to maintain protection and integrity of the device, and it is advised to implement the following requirements to secure IoT hardware components, where applicable: • Deploy a Hardware Root of Trust component, which helps in authenticating hardware, firmware, and software components before loading them. It also helps in establishing trust in the boot environment. • Include only essential physical external ports that are necessary for the IoT device to function and enable only trusted connections to access and function on the physical ports.	Functional	intersects with	Roots of Trust Protection	AST-18	Mechanisms exist to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data that can be used as a "roots of trust" basis for integrity verification.	5	
2-15-1	N/A	Utilize hardware that embeds cybersecurity functions at the component level, to maintain protection and integrity of the device, and it is advised to implement the following requirements to secure IoT hardware components, where applicable: • Deploy a Hardware Root of Trust component, which helps in authenticating hardware, firmware, and software components before loading them. It also helps in establishing trust in the boot environment. • Include only essential physical external ports that are necessary for the IoT device to function and enable only trusted connections to access and function on the physical ports.	Functional	intersects with	Identification & Justification of Ports, Protocols & Services	TDA-02.5	Mechanisms exist to require process owners to identify, document and justify the business need for the ports, protocols and other services necessary to operate their technology solutions.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
2-15-2	N/A	Define and implement steps for installing and setting up an IoT device and service. It is recommended that these steps are in alignment with cybersecurity best practices regarding the usability of the device and service such as but not limited to: • Apply secure configuration and hardening options that are applicable to the organization, such as disabling certain features or functionalities that would not be used by the organization. • Implement secure set up and configuration to the IoT device, in order to reduce the exposure to threats; such as ensuring all IoT devices and related applications/services don't contain default or hardcoded passwords, and to be unique and complex. • Implement cybersecurity tests prior to deploying the application in the production environment. • Periodically conduct cybersecurity tests before and after every new software release.	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
2-15-2	N/A	Define and implement steps for installing and setting up an IoT device and service. It is recommended that these steps are in alignment with cybersecurity best practices regarding the usability of the device and service such as but not limited to: • Apply secure configuration and hardening options that are applicable to the organization, such as disabling certain features or functionalities that would not be used by the organization. • Implement secure set up and configuration to the IoT device, in order to reduce the exposure to threats; such as ensuring all IoT devices and related applications/services don't contain default or hardcoded passwords, and to be unique and complex. • Implement cybersecurity tests prior to deploying the application in the production environment. • Periodically conduct cybersecurity tests before and after every new software release.	Functional	subset of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.	10	
2-15-2	N/A	Define and implement steps for installing and setting up an IoT device and service. It is recommended that these steps are in alignment with cybersecurity best practices regarding the usability of the device and service such as but not limited to: • Apply secure configuration and hardening options that are applicable to the organization, such as disabling certain features or functionalities that would not be used by the organization. • Implement secure set up and configuration to the IoT device, in order to reduce the exposure to threats; such as ensuring all IoT devices and related applications/services don't contain default or hardcoded passwords, and to be unique and complex. • Implement cybersecurity tests prior to deploying the application in the production environment. • Periodically conduct cybersecurity tests before and after every new software release.	Functional	intersects with	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity and data protection controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
2-15-3	N/A	Develop and implement a plan for the withdrawal of the IoT devices and services at the end of their lifecycle. Implement the following practices for establishing an end-of-life strategy for the IoT devices and services: • Develop a replacement plan, and an end-of-life plan for the IoT devices and services that have run out of support and/or no longer support the essential cybersecurity functions. Also include third-party components within the end-of-life plan. • Implement measures to securely dispose the data that was stored or being processed by the IoT devices/ service, as per organizational policies and regulations. • Maintain an audit log to monitor the IoT devices and services disposal process.	Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
2-15-3	N/A	Develop and implement a plan for the withdrawal of the IoT devices and services at the end of their lifecycle. Implement the following practices for establishing an end-of-life strategy for the IoT devices and services: • Develop a replacement plan, and an end-of-life plan for the IoT devices and services that have run out of support and/or no longer support the essential cybersecurity functions. Also include third-party components within the end-of-life plan. • Implement measures to securely dispose the data that was stored or being processed by the IoT devices/ service, as per organizational policies and regulations. • Maintain an audit log to monitor the IoT devices and services disposal process.	Functional	intersects with	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.	5	
3-1	Cybersecurity Resilience Aspects of Business Continuity Management (BCM)	To ensure the inclusion of IoT cybersecurity resiliency requirements within the overall business continuity management plan of the organization, in order to enhance the integrity of IoT devices and services during cybersecurity incidents.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
3-1-1	N/A	Define, document, approve, and implement cybersecurity resiliency requirements for maintaining the confidentiality, integrity and availability of IoT devices and associated components, as part of the business continuity management plan of the organization, and review them periodically. As well as implementing the following: • Develop resiliency requirements in consideration of how the disruption of an IoT device's essential functions, due to a cyberattack, could impact the business operations associated with it. • Implement necessary resilience measures that are proportionate to the intended usage of the device, while considering other components that are associated with the IoT system, service or device. • Ensure essential cybersecurity functions of IoT devices and services are capable of functioning locally in case of a network or power outage and can return to a desired state after the outage.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
3-1-1	N/A	Define, document, approve, and implement cybersecurity resiliency requirements for maintaining the confidentiality, integrity and availability of IoT devices and associated components, as part of the business continuity management plan of the organization, and review them periodically. As well as implementing the following: • Develop resiliency requirements in consideration of how the disruption of an IoT device's essential functions, due to a cyberattack, could impact the business operations associated with it. • Implement necessary resilience measures that are proportionate to the intended usage of the device, while considering other components that are associated with the IoT system, service or device. • Ensure essential cybersecurity functions of IoT devices and services are capable of functioning locally in case of a network or power outage and can return to a desired state after the outage.	Functional	intersects with	Resilience To Outages	EMB-08	Mechanisms exist to configure embedded technology to be resilient to data network and power outages.	5	
3-1-2	N/A	IoT Endpoint devices, especially gateway devices, shall be capable of enforcing cybersecurity over communication networks and protocols even in the case of a connectivity outage/disruption to the back-end network, where applicable.	Functional	intersects with	Resilience To Outages	EMB-08	Mechanisms exist to configure embedded technology to be resilient to data network and power outages.	5	
4-1	Third-Party Cybersecurity	To ensure the protection of the organizational assets against cybersecurity risks in the IoT devices, procured or operated by a third-party.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
4-1-1	N/A	Define, document, approve, and implement IoT cybersecurity requirements within contracts with supply chain partners and third-parties.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
4-1-2	N/A	Request manufacturers and service providers of IoT products and services to demonstrate the cybersecurity capabilities within their products and/or services, and implement 'Secure-by-Design' principles throughout the development lifecycle phases of IoT devices and services.	Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity and data protection controls, including any flow-down requirements to subcontractors.	5	
4-1-3	N/A	Request developers and manufacturers to provide a list of hardware and software components present in the IoT devices and services, to assist in better understanding and managing risk and patching any known vulnerabilities.	Functional	intersects with	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
4-1-4	N/A	Identify IoT information systems, components, and services provided by supply chain partners and third-parties, for inclusion in the overall risk assessment and risk mitigation procedures.	Functional	intersects with	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of technology assets that support more than one critical business function.	5	
4-1-5	N/A	Implement verification activities, through audits, testing and software certifications assurance, to ensure that all IoT third-party components meet the cybersecurity policies of the organizations and the requirements highlighted in their contract.	Functional	subset of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.	10	
4-1-5	N/A	Implement verification activities, through audits, testing and software certifications assurance, to ensure that all IoT third-party components meet the cybersecurity policies of the organizations and the requirements highlighted in their contract.	Functional	intersects with	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity and data protection controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
4-1-6	N/A	Review periodically IoT risk mitigation procedures and cybersecurity requirements, that are related to supply chain partners and third-party, to detect any unauthorized procedures.	Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	5	
4-1-6	N/A	Review periodically IoT risk mitigation procedures and cybersecurity requirements, that are related to supply chain partners and third-party, to detect any unauthorized procedures.	Functional	intersects with	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
4-2	Cloud Computing and Hosting Cybersecurity	To ensure implementation of cybersecurity requirements for cloud services that are used for IoT devices.	Functional	no relationship	N/A	N/A	N/A	N/A	No requirements to map to.
4-2-1	N/A	Define, document, approve, and implement cybersecurity requirements for cloud services hosting IoT services, as well as other cloud services that are specifically used for IoT devices, in addition to including applicable Cloud Cybersecurity Controls (CCC) and periodically review them.	Functional	subset of	Cloud Services	CLD-01	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	10	
4-2-1	N/A	Define, document, approve, and implement cybersecurity requirements for cloud services hosting IoT services, as well as other cloud services that are specifically used for IoT devices, in addition to including applicable Cloud Cybersecurity Controls (CCC) and periodically review them.	Functional	intersects with	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	5	
4-2-2	N/A	Implement adequate authorization, authentication, verification and encryption policies and techniques to secure the IoT devices that interact with the private/ self-hosted IoT cloud service and/ or other cloud service specifically being used for IoT devices.	Functional	intersects with	Cloud Security Architecture	CLD-02	Mechanisms exist to ensure the cloud security architecture supports the organization's technology strategy to securely design, configure and maintain cloud employments.	5	
4-2-3	N/A	Assess the cybersecurity posture of the cloud service provider and/ or managed service provider to ensure that their cybersecurity posture is in alignment with the organization's IoT cybersecurity policies and procedures.	Functional	subset of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.	10	
4-2-3	N/A	Assess the cybersecurity posture of the cloud service provider and/ or managed service provider to ensure that their cybersecurity posture is in alignment with the organization's IoT cybersecurity policies and procedures.	Functional	intersects with	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity and data protection controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
4-2-4	N/A	Establish procedures to facilitate cybersecurity audits, cybersecurity monitoring of IoT-specific data manipulation activities, and management of potential risks associated with existence of a multi-tenant environment in the cloud, as part of the organization's cloud computing and hosting cybersecurity requirements.	Functional	intersects with	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity and data protection controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
4-2-5	N/A	Embed provisions in the contractual agreements with cloud service providers and/ or managed service to obtain data stored on cloud platforms in a vendor-neutral format in case of (a planned or unplanned) exit of the cloud service provider and/ or managed service provider from the cloud services agreement.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	