NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference Document: Secure Controls Framework (SCF) version 2026.3
STRM Guidance: https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm/

Focal Document: Singapore - Cybersecurity Code of Practice for Critical Information Infrastructure (CCP CII) (2026)
Focal Document URL: https://www.csa.gov.sg/legislation/codes-of-practice
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-apac-sgp-ccp-cii-2026.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	Notes	Legacy SCF #
1.1.1	Citation and Commencement	This Code is the Cybersecurity Code of Practice for Critical Information Infrastructure (2026) and shall take effect from 29 July 2026, superseding previous versions of the Code.	Functional	No Relationship	N/A	N/A	N/A	0		
1.2.1	Glossary and Interpretation	In this Code, unless the context otherwise requires, the terms defined in the Glossary shall have the corresponding meaning. (See FDE for details)	Functional	Intersects With	Standardized Terminology	GOV-03.2	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5		SEA-02.1
1.2.2	Glossary and Interpretation	A reference in this Code to a "clause" shall, unless otherwise stated, be construed as a reference to the corresponding clause in this Code and shall include all sub-clauses within that clause.	Functional	No Relationship	N/A	N/A	N/A	0		
1.2.3	Glossary and Interpretation	A reference in this Code to "including" shall not be construed restrictively but shall mean "including without prejudice to the generality of the foregoing" and "including but without limitation".	Functional	No Relationship	N/A	N/A	N/A	0		
1.2.4	Glossary and Interpretation	Use of the singular is deemed to include the plural (and vice versa).	Functional	No Relationship	N/A	N/A	N/A	0		
1.2.5	Glossary and Interpretation	Unless otherwise stated, the provisions of this Code shall apply to the CII, and where specifically indicated to apply to systems that communicate with or connect to the CII that the CIIO own, operate, and/or control. For the avoidance of doubt , references such as "the CII" or "a CII" do not in any way restrict the application of this Code to other CII that the CIIO owns.	Functional	No Relationship	N/A	N/A	N/A	0		
1.2.6	Glossary and Interpretation	The provisions of this Code shall also apply to CII interconnected systems that the CIIO own, operate, and/or control, referring to computer systems that connect to or communicate with the CII, as illustrated in the diagram below. While enterprise systems fall outside the scope of this Code, CIIOs are encouraged to refer to Annex A, which provides guidance on strengthening the cybersecurity posture of the enterprise system by implementing the measures set out therein.	Functional	No Relationship	N/A	N/A	N/A	0		
1.2.7	Glossary and Interpretation	Clauses in this Code are prefaced with a preamble or include illustrations (presented in italicised font and without clause numbers). The preambles and illustrations are intended to provide additional information on the context, purpose, or application of the clauses they relate to. The preambles and illustrations do not form part of the measures that the CIIO is required to take under this Code and hence need not be included in the scope of any cybersecurity audits carried performed by the CIIO under section 15 of the Act.	Functional	No Relationship	N/A	N/A	N/A	0		
1.3.1	Purpose of this Code	This Code is intended to specify the minimum requirements that the CIIO shall implement to ensure the cybersecurity of its CII and CII interconnected systems.	Functional	No Relationship	N/A	N/A	N/A	0		
1.3.2	Purpose of this Code	The CIIO is expected to implement measures beyond those stipulated in this Code to further strengthen the cybersecurity of the CII, CII interconnected systems and the CIIO's enterprise environment based on the cybersecurity risk profile of the CIIO.	Functional	No Relationship	N/A	N/A	N/A	0		
1.4.1	Legal Effect of this Code	The CIIO must comply with this Code pursuant to section 35A(6) of the Act.	Functional	No Relationship	N/A	N/A	N/A	0		
1.4.2	Legal Effect of this Code	The Previous Version is superseded with effect from the Effective Date.	Functional	No Relationship	N/A	N/A	N/A	0		
1.4.3	Legal Effect of this Code	As this Code may be updated periodically, the CIIO shall ensure compliance with each release within the compliance timeframe specified by the Commissioner at the time of the release 's issuance. The CIIO must ensure compliance with this Code by the Compliance Date as specified in the Compliance Timeline section.	Functional	No Relationship	N/A	N/A	N/A	0		
1.4.4	Legal Effect of this Code	For Existing CII, during the period between the Effective Date and the Compliance Date (referred to below as the "transition period") , the CIIO minimally comply with the requirements of this Code as at the Previous Version.	Functional	No Relationship	N/A	N/A	N/A	0		
1.4.5	Legal Effect of this Code	The CIIO's obligations under this Code are in addition to its other obligations under the Act and other laws, and any relevant written directions or other codes of practice issued by the Commissioner under the Act.	Functional	No Relationship	N/A	N/A	N/A	0		
1.4.6	Legal Effect of this Code	If any provision of this Code is held to be unlawful, all other provisions shall remain in full force and effect.	Functional	No Relationship	N/A	N/A	N/A	0		
1.4.7	Legal Effect of this Code	Where the provisions specified in this Code are not met by a CIIO, the Commissioner may issue a direction in writing under section 12(1) of the Act to the CIIO for compliance with the relevant provision.	Functional	No Relationship	N/A	N/A	N/A	0		
1.5.1	Recurring Requirements	This Code includes clauses requiring certain acts to be performed on a recurring basis at fixed intervals (e.g. , a requirement to perform an act at least once every 12 months) referred as "recurring requirements". The relevant clauses prescribe the deadline for the first instance of the act. For subsequent instances, the deadline shall be counted from the date the previous instance was performed.	Functional	No Relationship	N/A	N/A	N/A	0		
1.5.2	Recurring Requirements	For Existing CII, in respect of recurring requirements that already applied to the CII under the Previous Version, the deadline for the first instance after the Effective Date shall continue from the date the previous instance was performed.	Functional	No Relationship	N/A	N/A	N/A	0		
1.6.1	Waiver	The Commissioner may waive the application of any specific provisions of this Code to a CIIO under section 35A (7) of the Act.	Functional	No Relationship	N/A	N/A	N/A	0		
1.6.2	Waiver	A CIIO can request for waiver from specific provisions of this Code under section 35A (7) of the Act by submitting a written request to the Commissioner with valid justifications and compensating controls supporting the request, that are in place or will be put in place to achieve the policy intent of the clause requirements.	Functional	Intersects With	Exception Management	GOV-04.2	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	3		GOV-02.1
1.6.2	Waiver	A CIIO can request for waiver from specific provisions of this Code under section 35A (7) of the Act by submitting a written request to the Commissioner with valid justifications and compensating controls supporting the request, that are in place or will be put in place to achieve the policy intent of the clause requirements.	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	3		BCD-07 RSK-06.2
1.6.3	Waiver	Any waiver, if granted by the Commissioner, shall be subject to such terms and conditions as the Commissioner may specify and may, without limitation, be for a fixed period or effective until the occurrence of a specific event.	Functional	No Relationship	N/A	N/A	N/A	0		
1.7.1	Amendment and Revocation	The Commissioner may, at any time, amend or revoke this Code under section 35(A)(b) of the Act.	Functional	No Relationship	N/A	N/A	N/A	0		
2.1.1	Remediation of Audit Findings	Where any audit identifies any non-compliance by a CIIO with the requirements specified in the Act or any codes of practice or standards of performance issued under the Act, the CIIO shall, unless the Commissioner indicates otherwise in writing, submit an audit finding remediation plan to the Commissioner within 30 working days from the date that the CIIO receives the audit report.	Functional	Intersects With	Non-Conformity Oversight	CPL-06	Mechanisms exist to identify and document instances of non-conformity with statutory, regulatory and/or contractual obligations, in order to develop appropriate risk mitigation actions.	5		CPL-01.1
2.1.1	Remediation of Audit Findings	Where any audit identifies any non-compliance by a CIIO with the requirements specified in the Act or any codes of practice or standards of performance issued under the Act, the CIIO shall, unless the Commissioner indicates otherwise in writing, submit an audit finding remediation plan to the Commissioner within 30 working days from the date that the CIIO receives the audit report.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and	5		IAO-05
2.1.2	Remediation of Audit Findings	The audit finding remediation plan shall:	Functional	Intersects With	Non-Conformity Corrective Action	CPL-06.1	Mechanisms exist to implement corrective action to remediate instances of non-conformity with applicable statutory, regulatory, and/or contractual compliance	5		CPL-02.3
2.1.2(a)	Remediation of Audit Findings	Detail the remediation actions which the CIIO will take to address each area of non- compliance;	Functional	Intersects With	Non-Conformity Corrective Action	CPL-06.1	Mechanisms exist to implement corrective action to remediate instances of non-conformity with applicable statutory, regulatory, and/or contractual compliance	5		CPL-02.3
2.1.2(b)	Remediation of Audit Findings	Set out the timeline(s) for implementing the actions stated in sub-clause (a); and	Functional	Intersects With	Non-Conformity Corrective Action	CPL-06.1	Mechanisms exist to implement corrective action to remediate instances of non-conformity with applicable statutory, regulatory, and/or contractual compliance	3		CPL-02.3

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
2.1.2(b)	Remediation of Audit Findings	Set out the timeline(s) for implementing the actions stated in sub-clause (a); and	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and	3		IAO-05
2.1.2(c)	Remediation of Audit Findings	Identify the person(s) or department(s) responsible for the execution and oversight of each remediation action.	Functional	Intersects With	Non-Conformity Corrective Action	CPL-06.1	Mechanisms exist to implement corrective action to remediate instances of non-conformity with applicable statutory, regulatory, and/or contractual compliance	3		CPL-02.3
2.1.2(c)	Remediation of Audit Findings	Identify the person(s) or department(s) responsible for the execution and oversight of each remediation action.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience	3		GOV-04
2.1.2(d)	Remediation of Audit Findings	Specify the internal governance process for monitoring implementation progress, including the frequency of updates to the CIIO's Board or equivalent governing body regarding the status of implementation of the actions stated in sub-clause (a).	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program	5		GOV-01.2
2.1.3	Remediation of Audit Findings	The Commissioner may, after consultation with the CIIO and where the Commissioner considers it appropriate, require the CIIO to revise its audit finding remediation plan and resubmit the revised audit finding remediation plan to the Commissioner within such timeframe as may be prescribed by the Commissioner.	Functional	Intersects With	Capabilities Deficiency Tracking	IAO-12	Mechanisms exist to govern identified deficiencies (e.g., Plan of Action and Milestones (POA&M) or similar methodology) that formally documents, at a minimum: (1) Deficiency tracking number; (2) Applicable security, compliance and/or resilience control; (3) Description of the deficiency(ies); (4) Risk associated with the deficiency(ies); (5) Source deficiency identification/detection; (6) Temporary compensating controls, if applicable; (7) Point of Contact (POC) (e.g., asset/process owner); (8) Resources required to conduct remediation actions; (9) Planned remedial actions to the deficiency(ies); (10) Proposed remediation timeline; and	3		IAO-05
2.1.4	Remediation of Audit Findings	The CIIO shall implement the audit finding remediation plan and complete all remediation actions within the timeframe(s) specified in the said plan, to the Commissioner's satisfaction, and at the CIIO's own cost. The CIIO shall update the Commissioner and CIIO's Board or equivalent governing body when each remediation action is completed.	Functional	Intersects With	Non-Conformity Corrective Action	CPL-06.1	Mechanisms exist to implement corrective action to remediate instances of non-conformity with applicable statutory, regulatory, and/or contractual compliance obligations.	5		CPL-02.3
2.1.4	Remediation of Audit Findings	The CIIO shall implement the audit finding remediation plan and complete all remediation actions within the timeframe(s) specified in the said plan, to the Commissioner's satisfaction, and at the CIIO's own cost. The CIIO shall update the Commissioner and CIIO's Board or equivalent governing body when each remediation action is completed.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	3		GOV-01.2
3.1.1	Board-Level Accountability	The CIIO shall ensure that its Board's (or equivalent governing body and/or risk committee) Terms of Reference or mandate includes overseeing the organisation's cybersecurity risk posture and provide strategic direction and guidance to Senior Management on the management of cyber risks.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-05.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for identifying, mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5		GOV-04.1
3.1.1	Board-Level Accountability	The CIIO shall ensure that its Board's (or equivalent governing body and/or risk committee) Terms of Reference or mandate includes overseeing the organisation's cybersecurity risk posture and provide strategic direction and guidance to Senior Management on the management of cyber risks.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-09	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5		GOV-01.1
3.1.2	Board-Level Accountability	The CIIO Board's accountability and direction shall be evidenced through a documented cyber resilience framework covering risk tolerance, risk mitigation, risk transfer and risk recovery, comprising the following: The update to the Board for para 3.1.2(a), (b), (c) and (d) shall be documented in Board minutes or equivalent written records;	Functional	Intersects With	Steering Committee & Program Oversight	GOV-09	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives, which meets formally and on a regular basis.	5		GOV-01.1
3.1.2	Board-Level Accountability	The CIIO Board's accountability and direction shall be evidenced through a documented cyber resilience framework covering risk tolerance, risk mitigation, risk transfer and risk recovery, comprising the following: The update to the Board for para 3.1.2(a), (b), (c) and (d) shall be documented in Board minutes or equivalent written records;	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and	5		RSK-01
3.1.2(a)	Board-Level Accountability	Risk Tolerance - Issue and maintain a cyber risk appetite statement that defines the CIIO's acceptable levels of cyber risk . Review the cyber risk appetite statement and acceptable levels of cyber risk at least once every 12 months, or as often as required based on the evolving cyber threat landscape.	Functional	Intersects With	Risk Tolerance	RSK-05.1	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5		RSK-01.3
3.1.2(a)	Board-Level Accountability	Risk Tolerance - Issue and maintain a cyber risk appetite statement that defines the CIIO's acceptable levels of cyber risk . Review the cyber risk appetite statement and acceptable levels of cyber risk at least once every 12 months, or as often as required based on the evolving cyber threat landscape.	Functional	Intersects With	Risk Appetite	RSK-05.3	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	8		RSK-01.5
3.1.2(b)	Board-Level Accountability	Risk Mitigation - Be informed of the CIIO's cybersecurity budget and resource allocation, and exercise oversight on whether the allocation is adequate to address the cyber risks at least once every 12 months, or as often as required based on the evolving cyber threat landscape.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-09	Mechanisms exist to align security, compliance and resilience capabilities with business requirements through a steering committee or advisory board, comprised of key cybersecurity, data protection and business executives.	3		GOV-01.1
3.1.2(b)	Board-Level Accountability	Risk Mitigation - Be informed of the CIIO's cybersecurity budget and resource allocation, and exercise oversight on whether the allocation is adequate to address the cyber risks at least once every 12 months, or as often as required based on the evolving cyber threat landscape.	Functional	Intersects With	Allocation of Resources	PRM-06	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	5		PRM-03
3.1.2(c)	Board-Level Accountability	Risk Transfer - Be informed of the CIIO's cyber risk transfer arrangements, including cyber insurance coverage and material third-party indemnities, and exercise oversight of the cyber risk transfer arrangements at least once every 12 months, or as often as required based on the evolving cyber threat landscape.	Functional	Intersects With	Risk Treatment Options	RSK-16.1	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings, including: (1) Mitigating the risk to an acceptable level; (2) Avoiding the risk (e.g., terminating the project); (3) Transferring the risk to a third party (e.g., insurance and service provider); or	5		RSK-06.3
3.1.2(d)	Board-Level Accountability	Risk Recovery - Be informed of the Business Continuity and Disaster Recovery strategy that defines the organisation's maximum tolerable downtime following a cyber incident or a disruption to the provision of essential services, and exercise oversight of the strategy at least once every 12 months, or as often as required based on the evolving cyber threat landscape.	Functional	Intersects With	Defined Operational Resilience Requirements	BCD-02.1	Mechanisms exist to define operational resilience requirements for Technology Assets, Applications, Services and/or Data (TAASD) to operate in a controlled and acceptable manner during: (1) Routine operations; and (2) Adverse conditions.	5		
3.1.2(d)	Board-Level Accountability	Risk Recovery - Be informed of the Business Continuity and Disaster Recovery strategy that defines the organisation's maximum tolerable downtime following a cyber incident or a disruption to the provision of essential services, and exercise oversight of the strategy at least once every 12 months, or as often as required based on the evolving cyber threat landscape.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-04.1	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5		BCD-01.4
3.1.3	Board-Level Accountability	The CIIO shall ensure that its Board (or equivalent governing body and/or risk committee) participates in the board cybersecurity training that covers, at a minimum, the strategic oversight and governance of cybersecurity risks, and regulatory compliance obligations under the Cybersecurity Act and other applicable legislation and codes of practice.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5		SAT-03
3.1.4	Board-Level Accountability	The CIIO shall ensure that such cybersecurity training is contextualised to the CIIO's operating environment, delivered by an internal or external subject matter expert, and conducted at least once every 12 months, or as often as required based on the evolving cyber threat landscape. Newly appointed Board members (or equivalent governing body and/or risk committee) shall complete the training within 12 months of their appointment and shall be supported through regular cybersecurity briefings in the interim. The CIIO shall maintain records of attendance and curriculum for all board-level cybersecurity training conducted.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5		SAT-03

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.1.4	Board-Level Accountability	The CIIO shall ensure that such cybersecurity training is contextualised to the CIIO's operating environment, delivered by an internal or external subject matter expert, and conducted at least once every 12 months, or as often as required based on the evolving cyber threat landscape. Newly appointed Board members (or equivalent governing body and/or risk committee) shall complete the training within 12 months of their appointment and shall be supported through regular cybersecurity briefings in the interim. The CIIO shall maintain records of attendance and curriculum for all board-level cybersecurity training conducted.	Functional	Intersects With	Security, Compliance & Resilience Training Records	SAT-10	Mechanisms exist to document, retain and monitor individual training activities, including: (1) Initial security, compliance and resilience awareness training; (2) Recurring awareness training; and (3) Technology Assets, Applications and/or Services (TAAS)-specific training.	5		SAT-04
3.1.5	Board-Level Accountability	The CIIO shall ensure that its Board (or equivalent governing body and/or risk committee) receives a cyber threat briefing at least once every 6 months, or as often as needed based on the evolving cybersecurity threat landscape, and the Board's guidance or instructions arising from the cyber threat briefing shall be documented in Board minutes or equivalent written records. Each briefing shall cover, at a minimum:	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5		GOV-01.2
3.1.5	Board-Level Accountability	The CIIO shall ensure that its Board (or equivalent governing body and/or risk committee) receives a cyber threat briefing at least once every 6 months, or as often as needed based on the evolving cybersecurity threat landscape, and the Board's guidance or instructions arising from the cyber threat briefing shall be documented in Board minutes or equivalent written records. Each briefing shall cover, at a minimum:	Functional	Intersects With	Cyber Threat Environment Situational Awareness	SAT-06	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5		SAT-03.6
3.1.5(a)	Board-Level Accountability	Cyber threats relevant to the CII, the CIIO organisation and to the CIIO's sector;	Functional	Intersects With	Threat Intelligence Reporting	THR-05	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.	3		THR-03.1
3.1.5(b)	Board-Level Accountability	Any threats actively targeting the CII, the CIIO organisation, and/or the CIIO's sector since the last briefing; and	Functional	Intersects With	Threat Intelligence Reporting	THR-05	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.	3		THR-03.1
3.1.5(c)	Board-Level Accountability	Implications of those threats for the CIIO's cyber risk posture, including any recommended changes to controls, risk appetite, cybersecurity budget or resource allocation.	Functional	Intersects With	Risk Monitoring	RSK-22	Mechanisms exist to monitor risk as an integral part of the continuous monitoring strategy, including: (1) The effectiveness of security, compliance and	3		RSK-11
3.1.5(c)	Board-Level Accountability	Implications of those threats for the CIIO's cyber risk posture, including any recommended changes to controls, risk appetite, cybersecurity budget or resource allocation.	Functional	Intersects With	Threat Intelligence Reporting	THR-05	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.	3		THR-03.1
3.2.1	Senior Management Responsibility	The CIIO shall ensure that at least one member of its senior management, or an individual working in or for the CIIO, possesses the knowledge and awareness necessary to manage cyber risks across the CII, its interconnected systems, and the CIIO's enterprise network, provide oversight of cybersecurity measures, and ensure their appropriate implementation. Where a senior management member or equivalent, e.g. a Chief Information Security Officer (CISO) is designated for this purpose, the CIIO shall ensure that the individual is vested with the authority and competencies required to effectively discharge their cybersecurity responsibilities.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience Program (SCRP).	8		GOV-04
3.2.1	Senior Management Responsibility	The CIIO shall ensure that at least one member of its senior management, or an individual working in or for the CIIO, possesses the knowledge and awareness necessary to manage cyber risks across the CII, its interconnected systems, and the CIIO's enterprise network, provide oversight of cybersecurity measures, and ensure their appropriate implementation. Where a senior management member or equivalent, e.g. a Chief Information Security Officer (CISO) is designated for this purpose, the CIIO shall ensure that the individual is vested with the authority and competencies required to effectively discharge their cybersecurity responsibilities.	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	5		HRS-03.2
3.2.2	Senior Management Responsibility	The CIIO shall ensure that the role of the senior management or the assigned individual working in or for the CIIO stated in 3.2.1 are set out in writing, and the responsibility for each of these roles is assigned to a person working in or for the CIIO. This document shall:	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience	8		GOV-04
3.2.2	Senior Management Responsibility	The CIIO shall ensure that the role of the senior management or the assigned individual working in or for the CIIO stated in 3.2.1 are set out in writing, and the responsibility for each of these roles is assigned to a person working in or for the CIIO. This document shall:	Functional	Intersects With	Defined Roles & Responsibilities	HRS-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8		HRS-03
3.2.2(a)	Senior Management Responsibility	Specify the organisational structure for persons involved in managing and ensuring the cybersecurity of the CIIO;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-05.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for identifying, mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5		GOV-04.1
3.2.2(b)	Senior Management Responsibility	Specify what each of these roles is authorised to do and/or approve. This should include, at a minimum, the following areas:	Functional	Intersects With	Defined Roles & Responsibilities	HRS-04	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5		HRS-03
3.2.2(b)i	Senior Management Responsibility	Incident reporting and escalation: the role(s) responsible for detecting and reporting cybersecurity incidents, the escalation process to senior management or the relevant authority, and the expected timelines for doing so.	Functional	Intersects With	Authoritative Chain of Command	GOV-05.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity for individuals and teams managing Technology Assets, Applications, Services and/or Data (TAASD)-	3		GOV-04.2
3.2.2(b)i	Senior Management Responsibility	Incident reporting and escalation: the role(s) responsible for detecting and reporting cybersecurity incidents, the escalation process to senior management or the relevant authority, and the expected timelines for doing so.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10
3.2.2(b)ii	Senior Management Responsibility	Incident investigation: the role(s) responsible for leading and conducting investigations into cybersecurity incidents.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-11	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5		IRO-07
3.2.2(b)iii	Senior Management Responsibility	Cyber risk trade-off decisions: the role(s) authorised to make decisions to accept, mitigate, or transfer identified cyber risks, and at what threshold such decisions require escalation or approval from senior management or to the Board or equivalent governing body and/or risk committee.	Functional	Intersects With	Executive Leadership Approval For Managing Material Risk	RSK-06.1	Mechanisms exist to obtain executive leadership approval for risk management decisions involving material risk.	5		RSK-13
3.2.2(b)iii	Senior Management Responsibility	Cyber risk trade-off decisions: the role(s) authorised to make decisions to accept, mitigate, or transfer identified cyber risks, and at what threshold such decisions require escalation or approval from senior management or to the Board or equivalent governing body and/or risk committee.	Functional	Intersects With	Risk Treatment Options	RSK-16.1	Mechanisms exist to select appropriate risk treatment options, based on applicable risk assessment findings, including: (1) Mitigating the risk to an acceptable level; (2) Avoiding the risk (e.g., terminating the project); (3) Transferring the risk to a third party (e.g., insurance and service provider); or	3		RSK-06.3
3.2.2(b)iv	Senior Management Responsibility	Policy and resource approval: the role(s) authorised to approve cybersecurity policies, plans and expenditures for the effective management of cyber risks across the CIIO.	Functional	Intersects With	Assigned Security, Compliance & Resilience Responsibilities	GOV-05	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide Security, Compliance & Resilience	3		GOV-04
3.2.2(b)iv	Senior Management Responsibility	Policy and resource approval: the role(s) authorised to approve cybersecurity policies, plans and expenditures for the effective management of cyber risks across the CIIO.	Functional	Intersects With	Allocation of Resources	PRM-06	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	3		PRM-03
3.2.2(c)	Senior Management Responsibility	Ensure that the organisational structure prevents conflicts of interest from arising in relation to decisions relevant to the cybersecurity of the CIIO; and	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5		HRS-11
3.2.2(d)	Senior Management Responsibility	Be formally approved by the CIIO personally (where the CIIO consists of one or more natural person) or by the relevant officers responsible for the management of the CIIO (where the CIIO is not a natural person).	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	3		GOV-02
3.2.3	Senior Management Responsibility	The CIIO shall ensure that senior management provides the Board with a cyber threat briefing at least once every 6 months, or more frequently as the evolving threat landscape warrants. Each briefing shall cover, at a minimum, the matters set out in clauses 3.1.5(a) to (c).	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	5		GOV-01.2
3.2.3	Senior Management Responsibility	The CIIO shall ensure that senior management provides the Board with a cyber threat briefing at least once every 6 months, or more frequently as the evolving threat landscape warrants. Each briefing shall cover, at a minimum, the matters set out in clauses 3.1.5(a) to (c).	Functional	Intersects With	Threat Intelligence Reporting	THR-05	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.	3		THR-03.1

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.2.4	Senior Management Responsibility	The CIIO shall ensure that senior management provides the Board with regular reports on the organisation's cybersecurity posture, risks and reportable incidents (in accordance with the National Cybersecurity Incident Reporting Framework) affecting the CII, its interconnected systems, and the CIIO's enterprise network. Such reports shall be provided at least once every 6 months, and promptly upon the occurrence of a reportable incidents or material changes to the CIIO's cyber risk profile. All reports and related deliberations shall be documented in Board 's minutes or equivalent written records.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
3.2.4	Senior Management Responsibility	The CIIO shall ensure that senior management provides the Board with regular reports on the organisation's cybersecurity posture, risks and reportable incidents (in accordance with the National Cybersecurity Incident Reporting Framework) affecting the CII, its interconnected systems, and the CIIO's enterprise network. Such reports shall be provided at least once every 6 months, and promptly upon the occurrence of a reportable incidents or material changes to the CIIO's cyber risk profile. All reports and related deliberations shall be documented in Board 's minutes or equivalent written records.	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	8		GOV-01.2
3.2.5	Senior Management Responsibility	The CIIO shall ensure that senior management allocates adequate resources and budget for cybersecurity, commensurate with the cyber risks facing the CII, its interconnected systems, and the CIIO's enterprise network. The adequacy of such resources and budget shall be reviewed at least once every 12 months or following any material change to the CIIO's cyber risk profile, and the outcomes of such reviews shall be documented.	Functional	Intersects With	Security, Compliance & Resilience Resource Management	PRM-05	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the Security, Compliance & Resilience Program (SCRP) and document all exceptions.	5		PRM-02
3.2.5	Senior Management Responsibility	The CIIO shall ensure that senior management allocates adequate resources and budget for cybersecurity, commensurate with the cyber risks facing the CII, its interconnected systems, and the CIIO's enterprise network. The adequacy of such resources and budget shall be reviewed at least once every 12 months or following any material change to the CIIO's cyber risk profile, and the outcomes of such reviews shall be documented.	Functional	Intersects With	Allocation of Resources	PRM-06	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	8		PRM-03
3.3.1	Cyber Trust Mark Certification	The CIIO shall be certified with Cyber Trust Mark Advocate (Tier 5) or its equivalent within 24 months of its designation as an owner of CII systems and ensure that its certification remain valid. For existing CIIO, the CIIO shall be certified with Cyber Trust Mark Advocate (Tier 5) or its equivalent by the date stipulated by CSA.	Functional	Intersects With	Conformity Assessment	CPL-04.1	Mechanisms exist to conduct assessments to demonstrate security, compliance and/or resilience capability conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	5		CPL-01.4
3.3.2	Cyber Trust Mark Certification	The scope of certification shall encompass the CIIO's governance, risk management, and enterprise-wide management of cybersecurity capabilities, system operational processes, and information systems and infrastructure that the organisation owns, operates, and/or controls, which are used to deliver its products and services.	Functional	Intersects With	Compliance Scope	CPL-03	Mechanisms exist to document and validate the scope of security, compliance and resilience controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5		CPL-01.2
3.3.3	Cyber Trust Mark Certification	The CIIO shall ensure that the audit firm it engages to perform the cybersecurity audit under Section 15 of the Act be certified with Cyber Trust Mark Advocate (Tier 5) or its equivalent.	Functional	Intersects With	Independent Assessors	CPL-08	Mechanisms exist to utilize independent assessors to evaluate security, compliance and resilience at planned intervals or when the Technology Asset, Application and/or Service (TAAS) undergoes significant changes.	3		CPL-03.1
3.4.1	Risk Management	The CIIO shall establish and implement a cybersecurity risk management framework that provides for the following:	Functional	Intersects With	Risk Management Program	RSK-02	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls that are aligned with: (1) The organization's Enterprise Risk Management (ERM); and	8		RSK-01
3.4.1(a)	Risk Management	Promotion of a "risk culture" that enables the organisation and its personnel to have open communications about risk, embrace learning from positive and negative experiences, make informed decisions about addressing risks, and carry out risk management efforts commensurate with defined risk appetites;	Functional	Intersects With	Risk Culture	RSK-04	Mechanisms exist to ensure teams are committed to a culture that considers and communicates technology-related risk.	8		RSK-12
3.4.1(b)	Risk Management	The roles and responsibilities of various persons responsible for managing cybersecurity risks to the CII and their governance structure, including their reporting lines and accountabilities;	Functional	Intersects With	Stakeholder Accountability Structure	GOV-05.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for identifying, mapping, measuring and managing Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5		GOV-04.1
3.4.1(b)	Risk Management	The roles and responsibilities of various persons responsible for managing cybersecurity risks to the CII and their governance structure, including their reporting lines and accountabilities;	Functional	Intersects With	Risk Owner	RSK-11	Mechanisms exist to identify a risk owner for each item in the risk register to ensure clear accountability for unremediated risks.	3		RSK-03.2
3.4.1(c)	Risk Management	Cybersecurity risk assessment methodology;	Functional	Intersects With	Risk Assessment Methodology	RSK-12	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient	8		RSK-04.2
3.4.1(d)	Risk Management	Processes for the monitoring, communication and reporting of cybersecurity risks in a timely manner - the CIIO's senior management must be given regular reports of cybersecurity risks to the CII so that they are kept aware of the risks and impact, are able to manage the risks, and can ensure that the necessary cybersecurity measures to address the risks are implemented;	Functional	Intersects With	Status Reporting To Governing Body	GOV-09.1	Mechanisms exist to provide governance oversight reporting and recommendations enabling executives to make decisions about matters considered material to the organization's Security, Compliance & Resilience Program (SCRP).	3		GOV-01.2
3.4.1(d)	Risk Management	Processes for the monitoring, communication and reporting of cybersecurity risks in a timely manner - the CIIO's senior management must be given regular reports of cybersecurity risks to the CII so that they are kept aware of the risks and impact, are able to manage the risks, and can ensure that the necessary cybersecurity measures to address the risks are implemented;	Functional	Intersects With	Risk Monitoring	RSK-22	Mechanisms exist to monitor risk as an integral part of the continuous monitoring strategy, including: (1) The effectiveness of security, compliance and resilience controls; (2) Changes to the organization's risk profile; and (3) Changes to Technology Assets, Applications and/or	5		RSK-11
3.4.1(e)	Risk Management	The organisation's cybersecurity risk appetite and thresholds or limits for residual risk; and	Functional	Intersects With	Risk Threshold	RSK-05.2	Mechanisms exist to define organizational risk threshold, the level of risk exposure above which risks are addressed and below which risks may be accepted.	5		RSK-01.4
3.4.1(e)	Risk Management	The organisation's cybersecurity risk appetite and thresholds or limits for residual risk; and	Functional	Intersects With	Risk Appetite	RSK-05.3	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	5		RSK-01.5
3.4.1(f)	Risk Management	Process hazard analysis methodology to reduce or remove the impact on safety due to hazardous events (applicable for a CII which is an OT system).	Functional	Intersects With	Safety Assessment	EMB-19	Mechanisms exist to evaluate the safety aspects of embedded technologies via a fault tree analysis, or similar method, to determine possible consequences of misuse, misconfiguration and/or failure.	5		EMB-15
3.4.2	Risk Management	The CIIO shall include the following steps in the cybersecurity risk assessment methodology:	Functional	Intersects With	Risk Assessment Methodology	RSK-12	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient	5		RSK-04.2
3.4.2(a)	Risk Management	Risk identification - identification of CII assets and cybersecurity threats, including threats identified from threat modelling, threat hunting, post-incident reviews of cybersecurity incidents, and the construction of risk scenarios;	Functional	Intersects With	Risk Identification	RSK-09	Mechanisms exist to identify and document risks, both internal and external.	8		RSK-03
3.4.2(a)	Risk Management	Risk identification - identification of CII assets and cybersecurity threats, including threats identified from threat modelling, threat hunting, post-incident reviews of cybersecurity incidents, and the construction of risk scenarios;	Functional	Intersects With	Threat Modeling	TDA-05.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	3		TDA-06.2
3.4.2(b)	Risk Management	Risk analysis - analysis of each risk scenario to determine the likelihood of occurrence and potential impact;	Functional	Intersects With	Risk Assessment	RSK-13	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	5		RSK-04
3.4.2(c)	Risk Management	Risk evaluation - determining, documenting and prioritising risks; and	Functional	Intersects With	Risk Assessment	RSK-13	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	5		RSK-04
3.4.2(d)	Risk Management	Risk response - treatment and monitoring of each risk to keep the risk level within the organisation's risk tolerance level.	Functional	Intersects With	Risk Response	RSK-16	Mechanisms exist to ensure proper risk response actions were performed to remediate findings from security, compliance and/or resilience-related: (1) Assessments; (2) Audits; and/or (3) Incidents.	5		RSK-06.1
3.4.2(d)	Risk Management	Risk response - treatment and monitoring of each risk to keep the risk level within the organisation's risk tolerance level.	Functional	Intersects With	Risk Monitoring	RSK-22	Mechanisms exist to monitor risk as an integral part of the continuous monitoring strategy, including: (1) The effectiveness of security, compliance and resilience controls; (2) Changes to the organization's risk profile; and (3) Changes to Technology Assets, Applications and/or Services (TAAS) that affect risk.	3		RSK-11
3.4.3	Risk Management	For CII which are OT systems, the CIIO shall also include non-digital engineering controls as mitigating controls in a cybersecurity risk assessment where applicable.	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	5		BCD-07 RSK-06.2
3.4.4	Risk Management	The CIIO shall maintain and keep updated a risk register for each CII. The risk register shall record information of all cybersecurity risks to the CII, including risks identified through cybersecurity risk assessments. The risk register shall include the following:	Functional	Intersects With	Risk Register	RSK-14	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	8		RSK-04.1

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.4.4(a)	Risk Management	Risk scenarios;	Functional	Intersects With	Risk Register	RSK-14	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	3		RSK-04.1
3.4.4(b)	Risk Management	Dates when the risk scenarios are identified;	Functional	Intersects With	Risk Register	RSK-14	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	3		RSK-04.1
3.4.4(c)	Risk Management	Existing measures in place to address the risk scenario;	Functional	Intersects With	Risk Register	RSK-14	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	3		RSK-04.1
3.4.4(d)	Risk Management	Current risk ratings;	Functional	Intersects With	Risk Register	RSK-14	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	3		RSK-04.1
3.4.4(e)	Risk Management	Risk treatment plan;	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-17.1	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	5		RSK-06.4
3.4.4(f)	Risk Management	Progress status of the treatment plan;	Functional	Intersects With	Risk Treatment Plan (RTP)	RSK-17.1	Mechanisms exist to formalize a Risk Treatment Plan (RTP) that applicable stakeholders will utilize to remediate identified risks according to a defined timeline.	3		RSK-06.4
3.4.4(g)	Risk Management	Residual risk ratings; and	Functional	Intersects With	Risk Register	RSK-14	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	3		RSK-04.1
3.4.4(h)	Risk Management	Risk owner.	Functional	Intersects With	Risk Owner	RSK-11	Mechanisms exist to identify a risk owner for each item in the risk register to ensure clear accountability for	5		RSK-03.2
3.4.5	Risk Management	The CIIO shall ensure that all cybersecurity risks listed in the risk register are reviewed and monitored regularly to ensure that the thresholds or limits for residual risk identified in accordance with clause 3.4.1(e) are not breached.	Functional	Intersects With	Risk Register	RSK-14	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5		RSK-04.1
3.4.5	Risk Management	The CIIO shall ensure that all cybersecurity risks listed in the risk register are reviewed and monitored regularly to ensure that the thresholds or limits for residual risk identified in accordance with clause 3.4.1(e) are not breached.	Functional	Intersects With	Risk Monitoring	RSK-22	Mechanisms exist to monitor risk as an integral part of the continuous monitoring strategy, including: (1) The effectiveness of security, compliance and resilience controls; (2) Changes to the organization's risk profile; and (3) Changes to Technology Assets, Applications and/or Services (TAAS) that affect risk.	5		RSK-11
3.5.1	Policies, Standards, Guidelines and Procedures	The CIIO shall establish and implement policies, standards, guidelines and procedures for managing cybersecurity risks and protecting CII against cybersecurity threats. The policies, standards, guidelines and procedures shall be:	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	8		GOV-02
3.5.1(a)	Policies, Standards, Guidelines and Procedures	Aligned with this Code, sector regulatory cybersecurity requirements, and applicable sectoral or national cybersecurity policies, standards, directions and procedures; and	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-02	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5		CPL-01
3.5.1(b)	Policies, Standards, Guidelines and Procedures	Published and communicated to all personnel and external parties who act on or have access to a CII.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-04	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5		GOV-02
3.5.2	Policies, Standards, Guidelines and Procedures	The CIIO shall review the policies, standards, guidelines and procedures against the CII cyber operating environment and cybersecurity threat landscape at least once every 12 months. The first instance of this review is to be completed no later than 12 months from the time the policies, standards, guidelines and procedures were established.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-04.1	Mechanisms exist to review the Security, Compliance & Resilience Program (SCRP), including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8		GOV-03
3.5.3	Policies, Standards, Guidelines and Procedures	The CIIO shall ensure that actual practices and implementation are consistent with the policies, standards, guidelines and procedures. Differences, if any, shall be resolved in a timely manner.	Functional	Intersects With	Operationalizing Security, Compliance & Resilience Capabilities	GOV-11	Mechanisms exist to compel data and/or process owners to operationalize security, compliance and resilience practices for Technology Assets, Applications, Services and/or Data (TAASD) under their control.	5		GOV-15
3.6.1	Security-by-Design	The CIIO shall adopt the Security-by-Design Framework 4 established by CSA to the extent that it applies to the CII 's system development lifecycle. Where there are parts of the Framework which do not apply to the CII 's system development lifecycle, the CIIO shall document how and why these parts are not applicable.	Functional	Intersects With	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.	5		PRM-07
3.6.1	Security-by-Design	The CIIO shall adopt the Security-by-Design Framework 4 established by CSA to the extent that it applies to the CII 's system development lifecycle. Where there are parts of the Framework which do not apply to the CII 's system development lifecycle, the CIIO shall document how and why these parts are not applicable.	Functional	Intersects With	Security, Compliance & Resilience Aware Design	SEA-02	Mechanisms exist to formally incorporate the organization's secure architecture principles into engineering, product and model design requirements to ensure security, compliance and resilience are built in by default and by design.	5		SEA-01.5
3.7.1	Cybersecurity Design Principles	The CIIO shall adopt the following principles in relation to its people, process and technologies to reduce cybersecurity risks to the CII:	Functional	Intersects With	Secure Engineering Principles	SEA-05	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5		SEA-01
3.7.1(a)	Cybersecurity Design Principles	The defence-in-depth principle to ensure that the security architecture of the CII includes multiple layers of security controls to prevent single point of failure;	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-06	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	8		NET-02 SEA-03
3.7.1(b)	Cybersecurity Design Principles	The least privilege principle to ensure that accounts and users are granted the least extent of access necessary to perform their required functions; and	Functional	Intersects With	Least Privilege	IAC-30	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.	8		IAC-21
3.7.1(c)	Cybersecurity Design Principles	The principle of segregation of duties to ensure that duties and responsibilities for critical functions relating to the CII are divided among different persons.	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	8		HRS-11
3.7.2	Cybersecurity Design Principles	The CIIO shall also adopt, to the extent possible, the following principles in relation to its people, process and technologies to reduce cybersecurity risks to the CII:	Functional	Intersects With	Secure Engineering Principles	SEA-05	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5		SEA-01
3.7.2(a)	Cybersecurity Design Principles	The defence-by-diversity principle to reduce the number of potential attack vectors by having diversity throughout the CII, including diversity in technology, manufacturers and suppliers of assets, communication pathways, etc.; and	Functional	Intersects With	Heterogeneity	SEA-22	Mechanisms exist to utilize a diverse set of technologies for system components to reduce the impact of technical vulnerabilities from the same Original Equipment Manufacturer (OEM).	8		SEA-13
3.7.2(a)	Cybersecurity Design Principles	The defence-by-diversity principle to reduce the number of potential attack vectors by having diversity throughout the CII, including diversity in technology, manufacturers and suppliers of assets, communication pathways, etc.; and	Functional	Intersects With	Supplier Diversity	TPM-06	Mechanisms exist to obtain security, compliance and resilience technologies from different suppliers to minimize supply chain risk.	3		TDA-03.1
3.7.2(b)	Cybersecurity Design Principles	The zero-trust principle 5 to ensure that each request for access to the CII is authenticated, authorised and validated for security configuration and posture before access is granted.	Functional	Intersects With	Zero Trust Architecture (ZTA)	NET-14	Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated	8		NET-01.1
3.8.1	Change Management	The CIIO shall establish a change management process to identify, authorise, implement and validate all changes made to the CII.	Functional	Intersects With	Change Management Program	CHG-02	Mechanisms exist to facilitate the implementation of a change management program.	8		CHG-01
3.8.1	Change Management	The CIIO shall establish a change management process to identify, authorise, implement and validate all changes made to the CII.	Functional	Intersects With	Configuration Change Control	CHG-03	Mechanisms exist to govern the technical configuration change control processes.	5		CHG-02
3.9.1	Use of Cloud Computing Systems and Services	The CIIO shall remain responsible and accountable for maintaining oversight of the cybersecurity of the CII and for managing cybersecurity risks to the CII, even when the CII is wholly or partly implemented on cloud computing systems.	Functional	Intersects With	Cloud Services	CLD-02	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	5		CLD-01
3.9.2	Use of Cloud Computing Systems and Services	The CIIO shall inform the Commissioner of any plans to implement the whole or any part of the CII on cloud computing systems, regardless of the deployment model (e.g., public cloud, private cloud or hybrid cloud) or service model (e.g., software as a service, platform as a service or infrastructure as a service) being considered.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
3.9.3	Use of Cloud Computing Systems and Services	The CIIO shall not implement the whole or any part of the CII on cloud computing systems unless:	Functional	Intersects With	Cloud Infrastructure Onboarding	CLD-03	Mechanisms exist to ensure cloud services are designed and configured so Technology Assets, Applications and/or Services (TAAS) are secured in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5		CLD-01.1
3.9.3	Use of Cloud Computing Systems and Services	The CIIO shall not implement the whole or any part of the CII on cloud computing systems unless:	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-13.1	Mechanisms exist to define instances that require a risk assessment to be performed.	5		RSK-04.3
3.9.3(a)	Use of Cloud Computing Systems and Services	It has conducted a cybersecurity risk assessment of the risks relating to and arising from the proposed implementation on cloud computing systems and ensured that the risks identified can be adequately addressed;	Functional	Intersects With	Risk Assessment	RSK-13	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	8		RSK-04
3.9.3(a)	Use of Cloud Computing Systems and Services	It has conducted a cybersecurity risk assessment of the risks relating to and arising from the proposed implementation on cloud computing systems and ensured that the risks identified can be adequately addressed;	Functional	Intersects With	Instances Requiring A Risk Assessment	RSK-13.1	Mechanisms exist to define instances that require a risk assessment to be performed.	5		RSK-04.3
3.9.3(b)	Use of Cloud Computing Systems and Services	The completed cybersecurity risk assessment is formally accepted by the CIIO and submitted to the Commissioner for review within 30 days of its completion; and	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	3		GOV-17
3.9.3(b)	Use of Cloud Computing Systems and Services	The completed cybersecurity risk assessment is formally accepted by the CIIO and submitted to the Commissioner for review within 30 days of its completion; and	Functional	Intersects With	Risk Assessment	RSK-13	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption,	3		RSK-04

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
3.9.3(c)	Use of Cloud Computing Systems and Services	Where it appears to the Commissioner that any part of the cybersecurity risk assessment was not carried out satisfactorily, the CIIO has completed rectification works to the Commissioner's satisfaction at the CIIO's own cost and within the timeframe(s) specified by the Commissioner.	Functional	Intersects With	Non-Conformity Corrective Action	CPL-06.1	Mechanisms exist to implement corrective action to remediate instances of non-conformity with applicable statutory, regulatory, and/or contractual compliance obligations.	3		CPL-02.3
3.9.4	Use of Cloud Computing Systems and Services	Where the CIIO is engaging or has engaged the services of a cloud computing service provider to assist in implementing the whole or any part of the CII on cloud computing systems, the CIIO shall ensure that the service provider appoints a person within Singapore authorised to accept service of any notice or legal process relating to the provision of services to the CIIO on the service provider's behalf.	Functional	Intersects With	Localized Representation	CPL-23	Mechanisms exist to appoint localized representation with a physical presence in the host country, as required by applicable laws and/or regulations.	5		CPL-08
3.9.4	Use of Cloud Computing Systems and Services	Where the CIIO is engaging or has engaged the services of a cloud computing service provider to assist in implementing the whole or any part of the CII on cloud computing systems, the CIIO shall ensure that the service provider appoints a person within Singapore authorised to accept service of any notice or legal process relating to the provision of services to the CIIO on the service provider's behalf.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-05
3.10.1	Outsourcing Management	The CIIO shall remain responsible and accountable for the cybersecurity of the CII even if it engages an external party to perform or assist in performing any functions, activities or operations in respect of the CII (referred to below as "outsourcing") .	Functional	Intersects With	Third-Party Management	TPM-02	Mechanisms exist to facilitate the implementation of third-party management controls.	5		TPM-01
3.10.2	Outsourcing Management	The CIIO shall establish processes to maintain oversight over all outsourced functions, activities or operations, in order to minimise cybersecurity exposure arising from such outsourcing.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
3.10.3	Outsourcing Management	The CII shall include terms in its agreement(s) with the external party to help ensure the cybersecurity of the CII and to reduce or mitigate the impact of any cybersecurity risks associated with the outsourcing, including risks associated with the external party's access to the CII and its operations, processing, storage, communications and other functions. This shall include terms stipulating:	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8		TPM-05
3.10.3(a)	Outsourcing Management	The type(s) of access that the external party has to the CII, taking into account the CIIO 's business requirements and the cybersecurity risk profile of the CII;	Functional	Intersects With	Third-Party Remote Access Governance	NET-30	Mechanisms exist to proactively control and monitor third-party accounts used to access, support, or maintain system components via remote access.	3		NET-14.6
3.10.3(a)	Outsourcing Management	The type(s) of access that the external party has to the CII, taking into account the CIIO 's business requirements and the cybersecurity risk profile of the CII;	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the	3		TPM-05
3.10.3(b)	Outsourcing Management	The obligations of the external party to protect the CII against cybersecurity threats and report cybersecurity incidents; and	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets,	3		TPM-05
3.10.3(b)	Outsourcing Management	The obligations of the external party to protect the CII against cybersecurity threats and report cybersecurity incidents; and	Functional	Intersects With	Security Compromise Notification Agreements	TPM-21.1	Mechanisms exist to compel External Service Providers (ESPs) to provide notification of actual or potential compromises in the supply chain that can potentially affect or have adversely affected Technology Assets, Applications and/or Services (TAAS) that the organization	5		TPM-05.1
3.10.3(c)	Outsourcing Management	The rights of the CIIO to commission an audit of the external party's cybersecurity posture in relation to the outsourced functions, activities or operations; or to require that the external party provide a copy of the audit report should the external party commission its own audit for these purposes.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	3		TPM-05
3.10.3(c)	Outsourcing Management	The rights of the CIIO to commission an audit of the external party's cybersecurity posture in relation to the outsourced functions, activities or operations; or to require that the external party provide a copy of the audit report should the external party commission its own audit for these purposes.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	3		TPM-08
3.10.4	Outsourcing Management	The CIIO shall establish processes for validating the external party's compliance with the terms required under clause 3.10.3 and any other terms in the agreement relating to cybersecurity.	Functional	Intersects With	Review of Third-Party Services	TPM-15	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for security, compliance and resilience controls.	5		TPM-08
3.10.5	Outsourcing Management	The CIIO shall ensure that it is able to renegotiate the terms of its agreements(s) with external parties in the event of new legal or regulatory requirements.	Functional	Intersects With	Third-Party Contract Requirements	TPM-14	Mechanisms exist to require contractual requirements for applicable security, compliance and resilience requirements with third-parties, reflecting the organization's needs to protect its Technology Assets,	3		TPM-05
4.1.1	Asset Management	The CIIO shall establish mechanisms and processes to identify all CII assets and maintain an inventory of the assets. The inventory shall include the following:	Functional	Intersects With	Asset Inventories	AST-04	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	8		AST-02
4.1.1	Asset Management	The CIIO shall establish mechanisms and processes to identify all CII assets and maintain an inventory of the assets. The inventory shall include the following:	Functional	Intersects With	Comprehensive Asset Inventory Management	AST-08	Mechanisms exist to maintain a dynamically updated inventory of Technology Assets, Applications, Services and/or Data (TAASD) that provides a highly contextualized understanding of every asset that is capable of providing operational visibility required to: (1) Detect anomalies; (2) Manage complex vulnerabilities; (3) Maintain compliance; and	5		
4.1.1(a)	Asset Management	Owner and/or operator of each CII asset;	Functional	Intersects With	Technology Assets, Applications, Services and/or Data (TAASD) Ownership Assignment	AST-07.1	Mechanisms exist to ensure Technology Assets, Applications, Services and/or Data (TAASD) ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for	5		AST-03
4.1.1(b)	Asset Management	Name and description of each CII asset;	Functional	Intersects With	Standardized Naming Convention	AST-03	Mechanisms exist to implement a scalable, standardized naming convention for Technology Assets, Applications, Services and/or Data (TAASD) that avoids asset naming conflicts.	3		AST-01.3
4.1.1(b)	Asset Management	Name and description of each CII asset;	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use;	3		AST-02
4.1.1(c)	Asset Management	Description of critical functions of each CII asset;	Functional	Intersects With	Identify Critical Assets	AST-05	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business	5		BCD-02
4.1.1(d)	Asset Management	Key person(s) responsible for the cybersecurity of each CII asset;	Functional	Intersects With	Accountability Information	AST-07.2	Mechanisms exist to formally document the name, position and/or role of individuals responsible/accountable for administering assets as part	5		AST-03.1
4.1.1(e)	Asset Management	The dependencies of each CII asset and the connections between each CII asset and any systems or networks (whether internal or external to the CII);	Functional	Intersects With	Asset-Service Dependencies	AST-06	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	5		AST-01.1
4.1.1(e)	Asset Management	The dependencies of each CII asset and the connections between each CII asset and any systems or networks (whether internal or external to the CII);	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and	3		AST-04
4.1.1(f)	Asset Management	Physical location of each CII asset;	Functional	Intersects With	Asset Inventories	AST-04	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	3		AST-02

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
4.1.1(g)	Asset Management	Outsourced service providers used to support each CII asset;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
4.1.1(h)	Asset Management	Cloud services used to support each CII asset.	Functional	Intersects With	Asset Inventories	AST-04	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	3		AST-02
4.1.1(h)	Asset Management	Cloud services used to support each CII asset.	Functional	Intersects With	Cloud Services	CLD-02	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	3		CLD-01
4.1.1(i)	Asset Management	Description of the internet links supporting the CII, including information on the distributed denial-of-service (DDoS) attack mitigation measures in place for these internet links; and	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use;	3		AST-02
4.1.1(i)	Asset Management	Description of the internet links supporting the CII, including information on the distributed denial-of-service (DDoS) attack mitigation measures in place for these internet links; and	Functional	Intersects With	Denial of Service (DoS) Protection	NET-21	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5		NET-02.1
4.1.1(j)	Asset Management	CII network topology diagram, including the CII network perimeter, and all external computers and computer systems that the CII interfaces with.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and	8		AST-04
4.1.2	Asset Management	The CIIO shall establish mechanisms and processes to identify systems that the CIIO owns, operates, and/or controls that interconnects with or communicates with the CII.	Functional	Intersects With	Asset Inventories	AST-04	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	5		AST-02
4.1.2	Asset Management	The CIIO shall establish mechanisms and processes to identify systems that the CIIO owns, operates, and/or controls that interconnects with or communicates with the CII.	Functional	Intersects With	Asset Discovery	AST-09	Automated mechanisms exist to perform asset discovery to identify Technology Assets, Applications and/or Services (TAAS) connected to organizational networks, including assets not present in existing inventories.	3		
4.1.3	Asset Management	The CIIO shall establish an inventory of systems that the CIIO owns, operates, and/or controls that interconnects with or communicates with the CII and update the inventory in a timely manner whenever there is a material change to any CII asset that requires corresponding updates to the systems that interconnects with or communicates with the CII.	Functional	Intersects With	Asset Inventories	AST-04	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	5		AST-02
4.1.3	Asset Management	The CIIO shall establish an inventory of systems that the CIIO owns, operates, and/or controls that interconnects with or communicates with the CII and update the inventory in a timely manner whenever there is a material change to any CII asset that requires corresponding updates to the systems that interconnects with or communicates with the CII.	Functional	Intersects With	Updates During Installations / Removals	AST-04.1	Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.	3		AST-02.1
4.1.4	Asset Management	The CIIO shall establish and maintain oversight for systems that the CIIO owns, operates, and/or controls that interconnects with or communicates with the CII.	Functional	Intersects With	Asset Governance	AST-02	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5		AST-01
5.1.1	Access Control	The CIIO shall ensure that access to the CII and between parts of the CII is restricted to authorised personnel, activities, processes and devices.	Functional	Intersects With	Identity & Access Management (IAM)	IAC-02	Mechanisms exist to facilitate the implementation of Identification and Access Management (IAM) controls.	5		IAC-01
5.1.1	Access Control	The CIIO shall ensure that access to the CII and between parts of the CII is restricted to authorised personnel, activities, processes and devices.	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5		IAC-20
5.1.2	Access Control	With respect to the CIIO's obligations under clause 5.1.1, the CIIO shall put in place authorisation and authentication controls for any access to the CII and between parts of the CII commensurate with the cybersecurity risk profile of the CII.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-03	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5		IAC-01.2
5.1.2	Access Control	With respect to the CIIO's obligations under clause 5.1.1, the CIIO shall put in place authorisation and authentication controls for any access to the CII and between parts of the CII commensurate with the cybersecurity risk profile of the CII.	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least privilege."	5		IAC-20
5.1.3	Access Control	The CIIO shall ensure that all external parties ' access to the CII are:	Functional	Intersects With	Access Enforcement	IAC-25	Mechanisms exist to enforce Logical Access Control (LAC) permissions that conform to the principle of "least	5		IAC-20
5.1.3	Access Control	The CIIO shall ensure that all external parties ' access to the CII are:	Functional	Intersects With	Third-Party Remote Access Governance	NET-30	Mechanisms exist to proactively control and monitor third-party accounts used to access, support, or maintain system components via remote access.	5		NET-14.6
5.1.3(a)	Access Control	Documented and pre-approved;	Functional	Intersects With	Management Approval For New or Changed Accounts	IAC-09	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	5		IAC-28.1
5.1.3(b)	Access Control	Supervised by the CIIO; and	Functional	Intersects With	Third-Party Personnel	HRS-13	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.	3		HRS-10
5.1.3(c)	Access Control	Performed on-site.	Functional	Intersects With	Remote Access	NET-26	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	3		NET-14
5.1.4	Access Control	The CIIO shall implement mechanisms to automatically terminate logon sessions after inactivity for a pre-defined time. If the logon sessions cannot be terminated, the CIIO shall monitor the logon sessions for anomalous activities and trigger an alert for investigation when any anomaly is detected.	Functional	Intersects With	Session Termination	CFG-04.5	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	5		IAC-25
5.1.4	Access Control	The CIIO shall implement mechanisms to automatically terminate logon sessions after inactivity for a pre-defined time. If the logon sessions cannot be terminated, the CIIO shall monitor the logon sessions for anomalous activities and trigger an alert for investigation when any anomaly is detected.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	3		MON-16
5.2.1	Account Management	With respect to accounts that have access to the CII, including any user, application, service or system account, the CIIO shall:	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	8		IAC-15
5.2.1(a)	Account Management	Grant to each account only the minimum privileges necessary for its assigned functions and uses;	Functional	Intersects With	Least Privilege	IAC-30	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.	8		IAC-21
5.2.1(b)	Account Management	Ensure that rights to install software are granted only to accounts that have been authorised to do so;	Functional	Intersects With	Restrict Roles Permitted To Install Software	CFG-12	Automated mechanisms exist to prevent the installation of software, unless the action is performed by a privileged user or service.	8		CFG-05 CFG-05.2
5.2.1(c)	Account Management	Ensure that shared user accounts are not created unless necessary for operating the CII;	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-21	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined	8		IAC-15.5
5.2.1(d)	Account Management	Establish mechanisms and processes to monitor the activities of each account, including behavioural patterns, for any anomalies and to trigger an alert for investigation when any anomaly is detected; and	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other	5		MON-16
5.2.1(e)	Account Management	Delete or disable any account that is no longer necessary or is inactive.	Functional	Intersects With	Disable Inactive Accounts	IAC-08.4	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	8		IAC-15.3

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
5.2.2	Account Management	The CIIO shall perform a review of all accounts that have access to the CII to evaluate the validity of accounts and to ensure that privileges assigned to each account are required to support operational or business activities. The CIIO shall perform this review at least once every 12 months. The first instance of this review is to be completed no later than 12 months after the Compliance Date.	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	5		IAC-15
5.2.2	Account Management	The CIIO shall perform a review of all accounts that have access to the CII to evaluate the validity of accounts and to ensure that privileges assigned to each account are required to support operational or business activities. The CIIO shall perform this review at least once every 12 months. The first instance of this review is to be completed no later than 12 months after the Compliance Date.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	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		IAC-17
5.3.1	Privileged Access Management	With respect to privileged accounts, the CIIO shall:	Functional	Intersects With	Privileged Account Management (PAM)	IAC-10	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications	8		IAC-16
5.3.1(a)	Privileged Access Management	Ensure that privileged access (i.e., administrative access) is granted only to selected accounts authorised to have such access;	Functional	Intersects With	Management Approval For Privileged Accounts	IAC-09.1	Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or	5		IAC-21.3
5.3.1(b)	Privileged Access Management	Ensure that privileged access is initiated from a cybersecurity hardened environment and transfer of data takes place over authorised connections;	Functional	Intersects With	Dedicated Administrative Machines	IAC-27	Mechanisms exist to restrict executing administrative tasks or tasks requiring elevated access to a dedicated machine.	5		IAC-20.4
5.3.1(c)	Privileged Access Management	Maintain an updated inventory of privileged accounts including details of the permissions and privileges assigned to each account;	Functional	Intersects With	Privileged Account Inventories	IAC-10.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational	8		IAC-16.1
5.3.1(d)	Privileged Access Management	Implement multi-factor authentication where privileged accounts are used to access the CII, and where privileges are to be escalated to the level of privileged access (e.g., where the user seeks to obtain additional permissions on a system or network after an initial log-in);	Functional	Intersects With	Multi-Factor Authentication (MFA) For Network Access to Privileged Accounts	IAC-37.5	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5		IAC-06.1
5.3.1(d)	Privileged Access Management	Implement multi-factor authentication where privileged accounts are used to access the CII, and where privileges are to be escalated to the level of privileged access (e.g., where the user seeks to obtain additional permissions on a system or network after an initial log-in);	Functional	Intersects With	Multi-Factor Authentication (MFA) For Local Access to Privileged Accounts	IAC-37.7	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5		IAC-06.3
5.3.1(e)	Privileged Access Management	Prohibit the sharing of privileged accounts used by network and system administrators, and any other personnel with privileged access, and establish processes to detect and remediate instances of account sharing.	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-21	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	3		IAC-15.5
5.3.1(e)	Privileged Access Management	Prohibit the sharing of privileged accounts used by network and system administrators, and any other personnel with privileged access, and establish processes to detect and remediate instances of account sharing.	Functional	Intersects With	Credential Sharing	IAC-23	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	5		IAC-19
5.3.1(f)	Privileged Access Management	Restrict use of "break glass" account(s) to emergency administrative use only where normal administrative access is unavailable. Access to such accounts shall be protected with access controls (e.g. "break glass" account password management process), logging and post-use review to ensure accountability.	Functional	Intersects With	Emergency Accounts	IAC-11	Mechanisms exist to establish and control "emergency access only" accounts.	8		IAC-15.9
5.3.1(f)	Privileged Access Management	Restrict use of "break glass" account(s) to emergency administrative use only where normal administrative access is unavailable. Access to such accounts shall be protected with access controls (e.g. "break glass" account password management process), logging and post-use review to ensure accountability.	Functional	Intersects With	Privileged Functions Logging	MON-14	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	3		MON-03.3
5.4.1	Domain Controller	The CIIO shall implement mechanisms and processes to:	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		MON-01
5.4.1	Domain Controller	The CIIO shall implement mechanisms and processes to:	Functional	Intersects With	Cross Domain Solution (CDS)	NET-41	Mechanisms exist to implement a Cross Domain Solution (CDS) to mitigate the specific security risks of accessing or transferring information between security domains.	3		NET-02.3
5.4.1(a)	Domain Controller	Monitor for changes to the trust relationships established between domains; and	Functional	Intersects With	Automated System Account Management	IAC-08.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	3		IAC-15.1
5.4.1(a)	Domain Controller	Monitor for changes to the trust relationships established between domains; and	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
5.4.1(b)	Domain Controller	Identify anomalies in the trust relationships and trigger an alert for investigation when any anomaly is detected	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other	5		MON-16
5.5.1	Network Segmentation	The CIIO shall segment the network architecture of the CII into different network segments based on their different security and risk levels.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network	8		NET-06
5.5.2	Network Segmentation	The CIIO shall limit any communications between the different network segments of a CII to only the minimum necessary for operating the CII.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5		NET-04
5.5.2	Network Segmentation	The CIIO shall limit any communications between the different network segments of a CII to only the minimum necessary for operating the CII.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network	5		NET-06
5.5.3	Network Segmentation	The CIIO shall:	Functional	Intersects With	Network Security Controls (NSC)	NET-02	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security	5		NET-01
5.5.3(a)	Network Segmentation	Implement network security mechanisms between the different network segments of the CII to detect and block malicious network traffic and to secure network communications; and	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		NET-03
5.5.3(a)	Network Segmentation	Implement network security mechanisms between the different network segments of the CII to detect and block malicious network traffic and to secure network communications; and	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-31	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5		NET-08
5.5.3(b)	Network Segmentation	Establish mechanisms and processes to isolate affected network segments of the CII in the event of a cybersecurity incident.	Functional	Intersects With	Dynamic Reconfiguration	IRO-07.3	Automated mechanisms exist to dynamically reconfigure system components as part of the incident response	5		IRO-02.3
5.5.3(b)	Network Segmentation	Establish mechanisms and processes to isolate affected network segments of the CII in the event of a cybersecurity incident.	Functional	Intersects With	Host Containment	NET-43	Automated mechanisms exist to enforce host containment protections that revoke or quarantine a host's access to the network.	3		NET-08.3
5.6.1	Network Security	The CIIO shall establish and implement network access control rules for the CII and perform periodic reviews to ensure they remain appropriate and up-to-date. The frequency of the review shall be commensurate with the cybersecurity risk profile of the CII.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	8		NET-04
5.6.1	Network Security	The CIIO shall establish and implement network access control rules for the CII and perform periodic reviews to ensure they remain appropriate and up-to-date. The frequency of the review shall be commensurate with the cybersecurity risk profile of the CII.	Functional	Intersects With	Human Reviews	NET-04.2	Mechanisms exist to enforce the use of human reviews for Access Control Lists (ACLs) and similar rulesets on a routine basis.	5		NET-04.6
5.6.2	Network Security	The CIIO shall ensure that the CII is not connected to any network outside of the CII except where necessary for operating the CII. Where such connections are necessary, the CIIO shall:	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		NET-03
5.6.2	Network Security	The CIIO shall ensure that the CII is not connected to any network outside of the CII except where necessary for operating the CII. Where such connections are necessary, the CIIO shall:	Functional	Intersects With	Limit Network Connections	NET-03.1	Mechanisms exist to limit the number of concurrent external network connections to its Technology Assets, Applications and/or Services (TAAS).	5		NET-03.1
5.6.2(a)	Network Security	Implement network security mechanisms between the CII and the network to detect and block malicious network traffic and to secure network communications; and	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.	3		NET-03
5.6.2(a)	Network Security	Implement network security mechanisms between the CII and the network to detect and block malicious network traffic and to secure network communications; and	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-31	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5		NET-08
5.6.2(b)	Network Security	Restrict the direction of data flow to only one-way if only one-way data flow is required for the operations of the CII.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5		NET-04
5.6.3	Network Security	The CIIO shall ensure that the CII is not connected to the internet except where required for operating the CII to deliver essential services. Where connection to the internet is required, the CIIO shall implement appropriate measures to mitigate and reduce cybersecurity risks arising from any such connection.	Functional	Intersects With	Direct Internet Access Restrictions	NET-03.4	Mechanisms exist to prohibit, or strictly-control, Internet access from sensitive and/or regulated data enclaves (secure zones).	8		NET-06.5
5.7.1	Remote Connection	The CIIO shall put in place effective cybersecurity measures for all remote connections to the CII to prevent and detect unauthorised access, and to validate that all such remote connections are authorised.	Functional	Intersects With	Remote Access	NET-26	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	8		NET-14
5.7.1	Remote Connection	The CIIO shall put in place effective cybersecurity measures for all remote connections to the CII to prevent and detect unauthorised access, and to validate that all such remote connections are authorised.	Functional	Intersects With	Remote Access Monitoring & Control	NET-26.4	Automated mechanisms exist to monitor and control remote access sessions.	5		NET-14.1
5.7.2	Remote Connection	The CIIO shall ensure that:	Functional	Intersects With	Remote Management of Embedded Technologies	EMB-15	Mechanisms exist to restrict remote management of embedded technologies by:	3		
5.7.2	Remote Connection	The CIIO shall ensure that:	Functional	Intersects With	Remote Access	NET-26	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5		NET-14
5.7.2(a)	Remote Connection	Remote connections to the CII are disabled except where necessary for operating the CII;	Functional	Intersects With	Remote Access	NET-26	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5		NET-14

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
5.7.2(b)	Remote Connection	Multi-factor authentication is required for the establishing a remote connection to the CII;	Functional	Intersects With	Multi-Factor Authentication (MFA)	IAC-37	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive and/or regulated data.	8		IAC-06
5.7.2(c)	Remote Connection	Remote connections to the CII have strong encryption and are made only through secured intermediary mechanisms;	Functional	Intersects With	Jump Server	AST-34	Mechanisms exist to conduct remote system administrative functions via a "jump box" or "jump server" that is located in a separate network zone to user	5		AST-27
5.7.2(c)	Remote Connection	Remote connections to the CII have strong encryption and are made only through secured intermediary mechanisms;	Functional	Intersects With	Remote Access Cryptographic Protections	NET-26.5	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	8		NET-14.2
5.7.2(d)	Remote Connection	Measures are put in place to ensure transmission security and message integrity over the remote connection;	Functional	Intersects With	Encrypting Data In Transit	CRY-05	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data in transit.	5		CRY-03
5.7.2(d)	Remote Connection	Measures are put in place to ensure transmission security and message integrity over the remote connection;	Functional	Intersects With	Integrity of Data In Transit	CRY-06	Cryptographic mechanisms exist to detect unauthorized changes to data in transit.	5		CRY-04
5.7.2(e)	Remote Connection	Files to be uploaded to the CII are scanned for malware before being uploaded; and	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04
5.7.2(f)	Remote Connection	Data flows over remote connections to the CII are limited to only the minimum necessary for performing the function required of the connection.	Functional	Intersects With	Data Flow Enforcement – Access Control Lists (ACLs)	NET-04	Mechanisms exist to implement and govern Access Control Lists (ACLs) to provide data flow enforcement that explicitly restrict network traffic to only what is authorized.	5		NET-04
5.8.1	Wireless Communication	The CIIO shall ensure that the CII is not connected to any wireless Local Area Network (LAN) except where necessary for operating the CII. Where any such connection is necessary, the CIIO shall ensure that:	Functional	Intersects With	Disable Wireless Networking	CFG-04.18	Mechanisms exist to disable unnecessary wireless networking capabilities that are internally embedded within system components prior to issuance to end users.	5		NET-15.2
5.8.1	Wireless Communication	The CIIO shall ensure that the CII is not connected to any wireless Local Area Network (LAN) except where necessary for operating the CII. Where any such connection is necessary, the CIIO shall ensure that:	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15
5.8.1(a)	Wireless Communication	Only authorised wireless LAN is used;	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15
5.8.1(b)	Wireless Communication	The connection has strong encryption; and	Functional	Intersects With	Wireless Networking Authentication & Encryption	NET-24.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	8		NET-15.1
5.8.1(c)	Wireless Communication	Only authorised devices (whether such devices are CII assets or otherwise) are allowed to connect to the wireless LAN.	Functional	Intersects With	Authorized To Connect	AST-10.1	Mechanisms exist to maintain a list of Technology Asset, Application and/or Service (TAAS) that are authorized to connect to organizational Technology Assets, Applications, Services and/or Data (TAASD).	5		AST-01.5
5.8.1(c)	Wireless Communication	Only authorised devices (whether such devices are CII assets or otherwise) are allowed to connect to the wireless LAN.	Functional	Intersects With	Network Access Control (NAC)	NET-16	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	5		AST-02.5
5.9.1	System Hardening	In respect of the following types of CII assets as they may be found in the CII, the CIIO shall establish and implement a security configuration baseline for each asset that is commensurate with the cybersecurity risk profile of the CII:	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	8		CFG-02
5.9.1(a)	System Hardening	Operating systems;	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	3		CFG-02
5.9.1(b)	System Hardening	Appliances;	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	3		CFG-02
5.9.1(c)	System Hardening	Consoles and workstations, including Human Machine Interfaces (HMI) and OT engineering workstations;	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	3		CFG-02
5.9.1(d)	System Hardening	Network devices;	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	3		CFG-02
5.9.1(e)	System Hardening	Servers, including alarm servers, OT historians and management servers;	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	3		CFG-02
5.9.1(f)	System Hardening	Software applications; and	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	3		CFG-02
5.9.1(g)	System Hardening	Any other CII asset or type of asset identified by the Commissioner.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	3		CFG-02
5.9.2	System Hardening	The security configuration baselines shall minimally address the following security practices:	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5		CFG-03
5.9.2	System Hardening	The security configuration baselines shall minimally address the following security practices:	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	5		CFG-02
5.9.2(a)	System Hardening	Account management - disable or remove default accounts, guest accounts, inactive accounts and unused accounts;	Functional	Intersects With	Disable Inactive Accounts	IAC-08.4	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	5		IAC-15.3
5.9.2(b)	System Hardening	Password and passphrase management - Default passwords shall be changed; passwords and passphrases shall be stored using in their hash forms;	Functional	Intersects With	Protection of Authenticators	IAC-14.2	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5		IAC-10.5
5.9.2(b)	System Hardening	Password and passphrase management - Default passwords shall be changed; passwords and passphrases shall be stored using in their hash forms;	Functional	Intersects With	Default Authenticators	IAC-14.4	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	5		IAC-10.8
5.9.2(c)	System Hardening	Application control - Disable services and remove applications that are not necessary for the operation of the CII;	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	8		CFG-03
5.9.2(d)	System Hardening	Port(s) and service(s) management - Enable only ports and services that are necessary for the operation of the CII;	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5		CFG-03
5.9.2(e)	System Hardening	Physical connection - Enable only external physical connections that are necessary for the operation of the CII;	Functional	Intersects With	Physically Disable or Remove Capabilities	CFG-05.1	Mechanisms exist to physically disable or remove unnecessary connection ports or input/output devices from technology assets at greater risk of device tampering.	5		END-12
5.9.2(f)	System Hardening	Malware protection - Install and update to the latest version of anti-malware software with the latest anti-malware signatures; and	Functional	Intersects With	Automatic Endpoint Protection Mechanism Updates	END-03.2	Automated mechanisms exist to update endpoint protection-related Technology Assets, Applications and/or Services (TAAS) when new releases are available, in	3		END-04.1 END-08.2
5.9.2(f)	System Hardening	Malware protection - Install and update to the latest version of anti-malware software with the latest anti-malware signatures; and	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	8		END-04
5.9.2(g)	System Hardening	Software upgrade and update - Timely upgrade and update of software and security patches .	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05
5.9.3	System Hardening	The CIIO shall review the security configuration baselines at least once every 12 months to ensure that the baselines remain effective in ensuring the cybersecurity of the CII. The first instance of this review is to be completed no later than 12 months from the time the baselines are established.	Functional	Intersects With	Baseline Configuration Reviews & Updates	CFG-07	Mechanisms exist to review and update secure baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and	8		CFG-02.1
5.9.4	System Hardening	The CIIO shall ensure that only authorised computing devices are used for the administration of the CII, and such devices are not used for other, non-administrative purposes.	Functional	Intersects With	Dedicated Administrative Machines	IAC-27	Mechanisms exist to restrict executing administrative tasks or tasks requiring elevated access to a dedicated machine.	8		IAC-20.4
5.10.1	Patch Management	The CIIO shall establish and implement a security patch management process that includes:	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-02	Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities.	5		VPM-01
5.10.1	Patch Management	The CIIO shall establish and implement a security patch management process that includes:	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05
5.10.1(a)	Patch Management	Monitoring the release of security patches for CII assets;	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	3		VPM-05

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
5.10.1(b)	Patch Management	Verifying the integrity of the security patches;	Functional	Intersects With	Software Patch Integrity	VPM-08.2	Mechanisms exist to ensure software and/or firmware patches are: (1) Obtained from trusted sources; and	8		VPM-05.8
5.10.1(c)	Patch Management	Testing security patches in a test environment that is similar to the CII production environment to ensure that the patches do not negatively affect the operations and cybersecurity of the CII;	Functional	Intersects With	Pre-Deployment Patch Testing	VPM-10	Mechanisms exist to perform due diligence on software and/or firmware update stability by conducting pre-production testing in a non-production environment.	8		VPM-05.6
5.10.1(d)	Patch Management	Prioritising the application of security patches based on the level of risk posed to the operations of the CII;	Functional	Intersects With	Vulnerability Ranking	VPM-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5		VPM-03
5.10.1(e)	Patch Management	Applying security patches in a timely manner to reduce cybersecurity vulnerabilities;	Functional	Intersects With	Time To Remediate / Benchmarks For Corrective Action	VPM-07	Mechanisms exist to track the effectiveness of remediation operations through metrics reporting.	5		VPM-05.3
5.10.1(e)	Patch Management	Applying security patches in a timely manner to reduce cybersecurity vulnerabilities;	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	3		VPM-05
5.10.1(f)	Patch Management	Monitoring and tracking the progress of patching;	Functional	Intersects With	Centralized Management of Flaw Remediation Processes	VPM-06.1	Mechanisms exist to centrally-manage the flaw remediation process.	3		VPM-05.1
5.10.1(g)	Patch Management	Applying compensating controls to mitigate and reduce cybersecurity risks in cases where a security patch cannot be applied; and	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	5		BCD-07 RSK-06.2
5.10.1(g)	Patch Management	Applying compensating controls to mitigate and reduce cybersecurity risks in cases where a security patch cannot be applied; and	Functional	Intersects With	Deferred Patching Decisions	VPM-09	Mechanisms exist to facilitate the deferral of software and/or firmware patches when the disadvantages of applying the patch outweigh the benefits.	5		VPM-04.3
5.10.1(h)	Patch Management	Rolling back the application of security patches where necessary.	Functional	Intersects With	Retention Of Previous Configurations	CFG-09	Mechanisms exist to retain previous versions of secure baseline configuration to support roll back.	3		CFG-02.3
5.10.2	Patch Management	The CIIO shall ensure that there is management oversight over the effectiveness of the security patch management processes.	Functional	Intersects With	Vulnerability & Patch Management Program (VPMP)	VPM-02	Mechanisms exist to facilitate the implementation and monitoring of risk-based vulnerability management capabilities.	5		VPM-01
5.11.1	Portable Computing Devices and Removable Storage Media	The CIIO shall establish processes to authorise and track the use of portable computing devices and removable storage media that connect to the CII.	Functional	Intersects With	Removable Media Security	DCH-21	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5		DCH-12
5.11.1	Portable Computing Devices and Removable Storage Media	The CIIO shall establish processes to authorise and track the use of portable computing devices and removable storage media that connect to the CII.	Functional	Intersects With	Access Control For Mobile Devices	IAC-35	Automated mechanisms exist to enforce access control requirements for the connection of mobile devices to organizational Technology Assets, Applications and/or Services (TAAS).	3		MDM-02
5.11.2	Portable Computing Devices and Removable Storage Media	The CIIO shall ensure that all such authorised portable computing devices adhere to a security configuration baseline that minimally addresses the security practices listed in clause 5.9.2, and satisfies any other security standards and requirements which the CIIO may have for such devices.	Functional	Intersects With	Secure Baseline Configurations	CFG-04	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted hardening standards.	3		CFG-02
5.11.2	Portable Computing Devices and Removable Storage Media	The CIIO shall ensure that all such authorised portable computing devices adhere to a security configuration baseline that minimally addresses the security practices listed in clause 5.9.2, and satisfies any other security standards and requirements which the CIIO may have for such devices.	Functional	Intersects With	Centralized Management Of Mobile Devices	MDM-02	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	5		MDM-01
5.11.3	Portable Computing Devices and Removable Storage Media	The CIIO shall ensure that authorised removable storage media are free of malware prior to connecting to the CII.	Functional	Intersects With	Removable Media Security	DCH-21	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5		DCH-12
5.11.3	Portable Computing Devices and Removable Storage Media	The CIIO shall ensure that authorised removable storage media are free of malware prior to connecting to the CII.	Functional	Intersects With	Malicious Code Protection (Antimalware)	END-04	Mechanisms exist to utilize antimalware, or similar technologies, to detect and eradicate malicious code.	5		END-04
5.11.4	Portable Computing Devices and Removable Storage Media	The CIIO shall ensure that sensitive information relating to the CII (including production data and system configuration information) that is stored in portable computing devices and removable storage media is secured with strong encryption.	Functional	Intersects With	Encrypting Storage Media	CRY-07.1	Cryptographic mechanisms exist to protect the confidentiality and integrity of sensitive and/or regulated data residing on storage media.	5		CRY-05.1
5.11.4	Portable Computing Devices and Removable Storage Media	The CIIO shall ensure that sensitive information relating to the CII (including production data and system configuration information) that is stored in portable computing devices and removable storage media is secured with strong encryption.	Functional	Intersects With	Full Device & Container-Based Encryption	MDM-04	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	5		MDM-03
5.12.1	Application Security	The CIIO shall ensure that only applications that are necessary for the operation and cybersecurity of the CII and that have been approved by the CIIO are used in the CII. The CIIO shall establish and maintain a list of such approved applications.	Functional	Intersects With	Approved Technologies	AST-10	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5		AST-01.4
5.12.1	Application Security	The CIIO shall ensure that only applications that are necessary for the operation and cybersecurity of the CII and that have been approved by the CIIO are used in the CII. The CIIO shall establish and maintain a list of such approved applications.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-14.1	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5		CFG-03.3
5.12.2	Application Security	The CIIO shall review the list of approved applications at least once every 12 months. The first instance of this review is to be completed no later than 12 months from the time the list is established.	Functional	Intersects With	Periodic Configuration Reviews	CFG-08	Mechanisms exist to periodically review Technology Assets, Applications and/or Services (TAAS) configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5		CFG-03.1
5.12.3	Application Security	The CIIO shall verify the integrity of applications before they are used in the CII.	Functional	Intersects With	Software / Firmware Integrity Verification	TDA-20.3	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware	5		TDA-14.1
5.12.4	Application Security	For a CII which is an IT system, the CIIO shall implement multi-tier architecture that separates the application and database tiers and implement security controls at each tier.	Functional	Intersects With	System Partitioning	SEA-07	Mechanisms exist to partition systems so that partitions reside in separate physical domains or environments.	5		SEA-03.1
5.12.5	Application Security	For a CII that includes web application systems, the CIIO shall reference the latest Open Web Application Security Project (OWASP) or equivalent application security guidelines when designing, developing and testing applications to minimise application security risks.	Functional	Intersects With	Web Security	WEB-02	Mechanisms exist to facilitate the implementation of an enterprise-wide web management policy, as well as associated standards, controls and procedures.	5		WEB-01
5.12.6	Application Security	For a CII that includes web application systems that are internet-facing, the CIIO shall also implement a Web Application Firewall (WAF) to monitor for, detect and block web application threats.	Functional	Intersects With	Web Application Firewall (WAF)	NET-34	Mechanisms exist to deploy Web Application Firewalls (WAFs) to provide defense-in-depth protection for application-specific threats.	8		WEB-03
5.12.7	Application Security	The CIIO shall ensure that compilers and debuggers are used in the CII only where necessary and only on devices authorised for such purposes. Compilers and debuggers shall be removed when they are no longer required.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5		CFG-03
5.13.1	Database Security	The CIIO shall ensure that only authorised accounts can connect to and query databases in a CII.	Functional	Intersects With	Database Access	IAC-25.2	Mechanisms exist to restrict access to databases containing sensitive and/or regulated data to only necessary Technology Assets, Applications and/or Services (TAAS) or those individuals whose job requires	8		IAC-20.2
5.13.2	Database Security	The CIIO shall ensure that duties relating to system administration and database administration for the CII are segregated and assigned to different persons.	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5		HRS-11
5.13.3	Database Security	The CIIO shall establish policies to secure databases in a CII, including policies for:	Functional	Intersects With	Database Management System (DBMS)	AST-35	Mechanisms exist to implement and maintain Database Management Systems (DBMSs), where applicable.	3		AST-28.1
5.13.3	Database Security	The CIIO shall establish policies to secure databases in a CII, including policies for:	Functional	Intersects With	Data Protection	DCH-02	Mechanisms exist to facilitate the implementation of data protection controls.	5		DCH-01
5.13.3(a)	Database Security	Securing data at rest;	Functional	Intersects With	Encrypting Data At Rest	CRY-07	Cryptographic mechanisms exist to prevent the unauthorized disclosure of data at rest.	5		CRY-05
5.13.3(a)	Database Security	Securing data at rest;	Functional	Intersects With	Database Encryption	CRY-08	Mechanisms exist to ensure that database servers utilize encryption to protect the confidentiality of the data within the databases.	5		CRY-05.3
5.13.3(b)	Database Security	Preventing data exfiltration; and	Functional	Intersects With	Data Loss Prevention (DLP)	DCH-40	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5		NET-17
5.13.3(b)	Database Security	Preventing data exfiltration; and	Functional	Intersects With	Prevent Unauthorized Exfiltration	NET-03.5	Automated mechanisms exist to prevent the unauthorized exfiltration of sensitive and/or regulated data across managed interfaces.	5		NET-03.5
5.13.3(c)	Database Security	Restricting access to sensitive data to authorised persons.	Functional	Intersects With	Restrict Sensitive / Regulated Data Access To Authorized Individuals	DCH-07.1	Mechanisms exist to control and restrict access to sensitive and/or regulated data on digital and non-digital media formats to authorized individuals.	5		DCH-03
5.13.3(c)	Database Security	Restricting access to sensitive data to authorised persons.	Functional	Intersects With	Access To Sensitive / Regulated Data	IAC-25.1	Mechanisms exist to limit access to sensitive and/or regulated data to only those individuals whose job	5		IAC-20.1
5.13.4	Database Security	The CIIO shall monitor databases in a CII for anomalous activities and trigger an alert for investigation when any anomaly is detected.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other	5		MON-16
5.13.4	Database Security	The CIIO shall monitor databases in a CII for anomalous activities and trigger an alert for investigation when any anomaly is detected.	Functional	Intersects With	Database Logging	MON-32	Mechanisms exist to ensure databases produce audit records that contain sufficient information to monitor	3		MON-03.7
5.13.5	Database Security	The CIIO shall monitor for bulk queries that exceed a predetermined threshold of data to be retrieved and trigger an alert for investigation when any such bulk query is detected.	Functional	Intersects With	Unusual Transactions	MON-16.1	Mechanisms exist to define "normal business activities" to identify anomalous transaction activities that can reduce the opportunity for sending (outbound) and/or receiving (inbound) hostile and/or fraudulent actions.	5		DCH-25.1
5.14.1	Vulnerability Assessment	The CIIO shall establish processes to identify and track cybersecurity vulnerabilities of the CII.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
5.14.2	Vulnerability Assessment	The CIIO shall remediate all cybersecurity vulnerabilities in a timely manner, with priority given to vulnerabilities that pose a greater risk to the security or operations of the CII.	Functional	Intersects With	Vulnerability Ranking	VPM-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5		VPM-03
5.14.2	Vulnerability Assessment	The CIIO shall remediate all cybersecurity vulnerabilities in a timely manner, with priority given to vulnerabilities that pose a greater risk to the security or operations of the CII.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02
5.14.3	Vulnerability Assessment	The CIIO shall conduct a vulnerability assessment of the CII:	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of	8		VPM-06
5.14.3(a)	Vulnerability Assessment	for a CII which is an IT system - at least once every 12 months, with the first instance to be completed by the Compliance Date; and	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of	3		VPM-06
5.14.3(b)	Vulnerability Assessment	for a CII which is an OT system - at least once every 24 months, with the first instance to be completed no later than 12 months after the Compliance Date.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	3		VPM-06
5.14.4	Vulnerability Assessment	The CIIO shall also conduct a vulnerability assessment for relevant CII assets after implementing any major system changes to the CII. Major system changes include commissioning new systems to be connected to the CII, implementing new application modules, system upgrades and technology refresh.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06
5.14.5	Vulnerability Assessment	The CIIO shall, if requested by the Commissioner, submit a copy of the report of any vulnerability assessment , along with the CIIO's plans for remediating each vulnerability, to the Commissioner within 30 working days of receiving the request.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
5.15.1	Penetration Testing	The CIIO shall conduct a penetration test on the CII:	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	8		VPM-07
5.15.1(a)	Penetration Testing	For a CII which is an IT system - at least once every 12 months, with the first instance to be completed by the Compliance Date; and	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	3		VPM-07
5.15.1(b)	Penetration Testing	For a CII which is an OT system - at least once every 24 months, with the first instance to be completed no later than 12 months after the Compliance Date.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	3		VPM-07
5.15.2	Penetration Testing	The CIIO shall also conduct penetration tests on relevant CII assets after implementing any major system changes to the CII. Major system changes include commissioning any new systems to be connected to the CII, implementing new application modules, system upgrades and technology refresh.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		VPM-07
5.15.3	Penetration Testing	The CIIO shall ensure that third-party penetration testing service providers and their penetration testers who are performing penetration tests on a CII possess industry-recognised accreditations and certifications respectively, for example CREST 6 or equivalent accreditations and certifications:	Functional	Intersects With	Independent Penetration Agent or Team	VPM-19	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5		VPM-07.1
5.15.3(a)	Penetration Testing	Penetration testers performing the penetration tests must have industry-recognised penetration testing certification to demonstrate assurance of their knowledge and practical skills.	Functional	Intersects With	Competency Requirements for Security, Compliance &	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	3		HRS-03.2
5.15.3(a)	Penetration Testing	Penetration testers performing the penetration tests must have industry-recognised penetration testing certification to demonstrate assurance of their knowledge and practical skills.	Functional	Intersects With	Independent Penetration Agent or Team	VPM-19	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	3		VPM-07.1
5.15.3(b)	Penetration Testing	Service providers must have industry-recognised accreditation to demonstrate assurance of their policies and procedures in penetration testing service, reporting and data handling, and due diligence in hiring of ethical penetration testers.	Functional	Intersects With	Third-Party Risk Assessments & Approvals	TPM-10	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	3		TPM-04.1
5.15.3(b)	Penetration Testing	Service providers must have industry-recognised accreditation to demonstrate assurance of their policies and procedures in penetration testing service, reporting and data handling, and due diligence in hiring of ethical penetration testers.	Functional	Intersects With	Independent Penetration Agent or Team	VPM-19	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	3		VPM-07.1
5.15.4	Penetration Testing	The CIIO shall ensure that all penetration tests by third-party service providers are conducted under supervision of the CIIO to ensure that activities carried out by the service providers are within the intended scope of the penetration test and do not disrupt CII operations.	Functional	Intersects With	Independent Penetration Agent or Team	VPM-19	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5		VPM-07.1
5.15.5	Penetration Testing	The CIIO shall, if requested by the Commissioner, submit a copy of the report of any completed penetration test , along with the CIIO's remediation plans, to the Commissioner within 30 working days of receiving the request.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
5.16.1	Adversarial Attack Simulation	The CIIO shall establish a red teaming or purple teaming attack simulation plan which identifies, among other things:	Functional	Intersects With	Red Team Exercises	VPM-21	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	5		VPM-10
5.16.1(a)	Adversarial Attack Simulation	Objectives to be achieved;	Functional	Intersects With	Red Team Exercises	VPM-21	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	3		VPM-10
5.16.1(b)	Adversarial Attack Simulation	Key stakeholders including red team, blue team and management team;	Functional	Intersects With	Red Team Exercises	VPM-21	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	3		VPM-10
5.16.1(c)	Adversarial Attack Simulation	Assessment methodology, including planning and attack preparation, attack execution, clean-up and containment, blue team report and reconciliation, recommendations and remediation;	Functional	Intersects With	Red Team Exercises	VPM-21	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	3		VPM-10
5.16.1(d)	Adversarial Attack Simulation	Rules of engagement (only for red teaming);	Functional	Intersects With	Red Team Exercises	VPM-21	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	3		VPM-10
5.16.1(e)	Adversarial Attack Simulation	Mitigation measures to minimise potential business impact or disruption; and	Functional	Intersects With	Red Team Exercises	VPM-21	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	3		VPM-10
5.16.1(f)	Adversarial Attack Simulation	Recovery plan.	Functional	Intersects With	Red Team Exercises	VPM-21	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	3		VPM-10
5.16.2	Adversarial Attack Simulation	The CIIO shall conduct a red teaming or purple teaming attack simulation on its CII at least once every 24 months to test and validate the effectiveness of its cybersecurity measures against prevalent cybersecurity threats. The first instance of the attack simulation is to be completed no later than 12 months after the Compliance Date.	Functional	Intersects With	Red Team Exercises	VPM-21	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.	8		VPM-10
5.16.3	Adversarial Attack Simulation	The CIIO shall, if requested by the Commissioner, submit a copy of the report of any completed red teaming or purple teaming attack simulation, along with the CIIO's remediation plans, to the Commissioner within 30 working days of receiving the request.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
5.17.1	Cryptographic Key Management	The CIIO shall ensure that all cryptographic keys for the CII are protected against unauthorised access.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
5.17.1	Cryptographic Key Management	The CIIO shall ensure that all cryptographic keys for the CII are protected against unauthorised access.	Functional	Intersects With	Control & Distribution of Cryptographic Keys	CRY-10.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and	3		CRY-09.4
5.17.2	Cryptographic Key Management	The CIIO shall establish and implement mechanisms and processes to track and manage the lifecycle of cryptographic keys. The CIIO shall review these mechanisms and processes at least once every 12 months to ensure their continued effectiveness. The first instance of this review is to be completed no later than 12 months from the time the mechanisms and processes are implemented.	Functional	Intersects With	Cryptographic Management	CRY-03	Mechanisms exist to govern assets involved in providing cryptographic protections according to the organization's configuration management processes.	3		CHG-02.5
5.17.2	Cryptographic Key Management	The CIIO shall establish and implement mechanisms and processes to track and manage the lifecycle of cryptographic keys. The CIIO shall review these mechanisms and processes at least once every 12 months to ensure their continued effectiveness. The first instance of this review is to be completed no later than 12 months from the time the mechanisms and processes are implemented.	Functional	Intersects With	Cryptographic Key Management	CRY-10	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5		CRY-09
6.1.1	Logging	The CIIO shall generate, collect and store logs of the following:	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		MON-01
6.1.1	Logging	The CIIO shall generate, collect and store logs of the following:	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the	5		MON-03

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
6.1.1(a)	Logging	All access and attempts to access the CII and the activities during such access, including application and database activities, and access to data in the CII;	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the	5		MON-03
6.1.1(a)	Logging	All access and attempts to access the CII and the activities during such access, including application and database activities, and access to data in the CII;	Functional	Intersects With	Database Logging	MON-32	Mechanisms exist to ensure databases produce audit records that contain sufficient information to monitor database activities.	3		MON-03.7
6.1.1(b)	Logging	Network connections between the CII and networks outside of the CII;	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-22	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5		MON-01.3
6.1.1(c)	Logging	Network connections within the CII;	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-22	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	3		MON-01.3
6.1.1(d)	Logging	Remote connections to the CII; and	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-22	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	3		MON-01.3
6.1.1(d)	Logging	Remote connections to the CII; and	Functional	Intersects With	Remote Access Monitoring & Control	NET-26.4	Automated mechanisms exist to monitor and control remote access sessions.	3		NET-14.1
6.1.1(e)	Logging	Connections between the CII and wireless LAN.	Functional	Intersects With	Wireless Network Monitoring	MON-26	Mechanisms exist to monitor wireless network segments for: (1) Rogue wireless devices; and	5		MON-01.5
6.1.2	Logging	The CIIO shall also generate, collect and store the following categories of logs to provide visibility of network activities within the CII and between the CII and networks outside of the CII:	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the	5		MON-03
6.1.2	Logging	The CIIO shall also generate, collect and store the following categories of logs to provide visibility of network activities within the CII and between the CII and networks outside of the CII:	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-22	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5		MON-01.3
6.1.2(a)	Logging	Network Firewall logs;	Functional	Intersects With	Verbosity Logging for Boundary Devices	MON-31	Mechanisms exist to verbosely log all traffic (both allowed and blocked) arriving at network boundary devices, including firewalls, Intrusion Detection / Prevention Systems (IDS/IPS) and inbound and outbound proxies.	5		MON-03.4
6.1.2(b)	Logging	Domain Name System (DNS) logs;	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the	3		MON-03
6.1.2(c)	Logging	Web Proxy logs; and	Functional	Intersects With	Proxy Logging	MON-22.1	Mechanisms exist to log all Internet-bound requests, in order to identify prohibited activities and assist incident handlers with identifying potentially compromised	5		MON-01.9
6.1.2(d)	Logging	Network Intrusion Detection/Prevention System (NIDS/NIPS) logs.	Functional	Intersects With	Network Intrusion Detection & Prevention Systems (NIDS & NIPS) Monitoring	MON-23	Mechanisms exist to monitor Network Intrusion Detection / Prevention Systems (NIDS / NIPS) technologies on critical systems, key network segments and network choke points.	5		MON-01.1
6.1.3	Logging	The CIIO shall provide any such logs referred to in clause 6.1.2 as may be required by the Commissioner for threat monitoring, threat analysis, threat alerts, and incident response.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory	3		GOV-17
6.1.3	Logging	The CIIO shall provide any such logs referred to in clause 6.1.2 as may be required by the Commissioner for threat monitoring, threat analysis, threat alerts, and incident response.	Functional	Intersects With	Sharing of Event Logs & Security-Relevant Telemetry	MON-36	Mechanisms exist to share event logs and security-relevant telemetry with third-party organizations based on specific cross-organizational sharing agreements.	5		MON-14.1
6.1.4	Logging	The CIIO shall ensure that the logs generated, collected, and stored under clauses 6.1.1 and 6.1.2:	Functional	Intersects With	System Generated Event Logs & Security-Relevant Telemetry	MON-04	Mechanisms exist to generate, monitor, correlate and respond to event logs and security-relevant telemetry from physical, cybersecurity, data protection and supply chain activities to achieve integrated situational awareness.	5		MON-01.4
6.1.4(a)	Logging	Use a consistent time source;	Functional	Intersects With	Time Stamps	MON-11	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to use an authoritative time source to generate time stamps for event logs and security-relevant telemetry.	5		MON-07
6.1.4(a)	Logging	Use a consistent time source;	Functional	Intersects With	Synchronization With Authoritative Time Source	MON-11.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	5		MON-07.1
6.1.4(b)	Logging	Are protected against unauthorised access, modification and deletion;	Functional	Intersects With	Protection of Event Logs & Security-Relevant Telemetry	MON-12	Mechanisms exist to protect event logs, security-relevant telemetry and audit tools from unauthorized access, modification and deletion.	8		MON-08
6.1.4(c)	Logging	Are stored for a minimum period of 12 months after the date of the event to which the log relates;	Functional	Intersects With	Event Log & Security-Relevant Telemetry Retention	MON-13	Mechanisms exist to retain event logs and security-relevant telemetry 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	8		MON-10
6.1.4(d)	Logging	Have a log file structure (i.e., the arrangement of data fields within each log file) that facilitates analysis and sharing of logs; and	Functional	Intersects With	Content of Event Logs	MON-09	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the	3		MON-03
6.1.4(d)	Logging	Have a log file structure (i.e., the arrangement of data fields within each log file) that facilitates analysis and sharing of logs; and	Functional	Intersects With	Logging Syntax	TDA-11.4	Mechanisms exist to require system developers to use an industry-defined secure logging format to generate event logs for specified event types at organization-defined level	3		TDA-02.14
6.1.4(e)	Logging	Are governed by a log retention policy to facilitate investigations into cybersecurity incidents, the conduct of threat hunting, and any other purposes relating to the cybersecurity of the CII.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Retention	MON-13	Mechanisms exist to retain event logs and security-relevant telemetry 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	5		MON-10
6.2.1	Monitoring and Detection	The CIIO shall establish and implement mechanisms and processes for the purposes of:	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	8		MON-01
6.2.1(a)	Monitoring and Detection	Monitoring and detecting all cybersecurity events in respect of the CII;	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		MON-01
6.2.1(a)	Monitoring and Detection	Monitoring and detecting all cybersecurity events in respect of the CII;	Functional	Intersects With	Event Log & Security-Relevant Telemetry Monitoring	MON-03	Mechanisms exist to review event logs and security-relevant telemetry on an ongoing basis and escalate incidents in accordance with established timelines and	5		MON-01.8
6.2.1(b)	Monitoring and Detection	Collecting and storing records of all such cybersecurity events (including, where available, logs relating to the cybersecurity event);	Functional	Intersects With	Centralized Collection of Event Logs & Security-Relevant Telemetry	MON-05	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of event logs and security-relevant	5		MON-02
6.2.1(c)	Monitoring and Detection	Analysing all such cybersecurity events, including correlating between cybersecurity events, and determining whether there is or has been any cybersecurity incident; and	Functional	Intersects With	Event Log & Security-Relevant Telemetry Analysis & Triage	MON-05.2	Mechanisms exist to ensure event log and security-relevant telemetry reviews include analysis and triage practices that integrate with the organization's established incident response processes.	5		MON-17
6.2.1(c)	Monitoring and Detection	Analysing all such cybersecurity events, including correlating between cybersecurity events, and determining whether there is or has been any cybersecurity incident; and	Functional	Intersects With	Correlate Monitoring Information	MON-08	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational	5		MON-02.1
6.2.1(d)	Monitoring and Detection	Triggering applicable incident reporting, response and recovery plans if there is or has been any cybersecurity incident.	Functional	Intersects With	Incident Response Operations	IRO-02	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-	5		IRO-01
6.2.2	Monitoring and Detection	For the purposes of monitoring and detecting cybersecurity events, the mechanisms and processes established by the CIIO shall include:	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		MON-01
6.2.2	Monitoring and Detection	For the purposes of monitoring and detecting cybersecurity events, the mechanisms and processes established by the CIIO shall include:	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other	5		MON-16
6.2.2(a)	Monitoring and Detection	Scanning for indicators of compromise (IOCs), including IP addresses, Uniform Resource Locator (URL), domains and hashes;	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-05	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential	5		IRO-03
6.2.2(a)	Monitoring and Detection	Scanning for indicators of compromise (IOCs), including IP addresses, Uniform Resource Locator (URL), domains and hashes;	Functional	Intersects With	Monitoring for Indicators of Compromise (IOC)	MON-17	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	8		MON-11.3

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
6.2.2(b)	Monitoring and Detection	Establishing the normal day-to-day operational activities and network traffic in the CII, and using this as a baseline against which the CIIO is to monitor for deviations and anomalous activities; and	Functional	Intersects With	Behavioral Baselining	THR-09	Automated mechanisms exist to establish behavioral baselines that capture information about user and entity behavior to enable dynamic threat discovery.	8		THR-11
6.2.2(c)	Monitoring and Detection	Ensuring that alerts for further investigation are triggered for all deviations and anomalous activities that are detected.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other	5		MON-16
6.2.3	Monitoring and Detection	The CIIO shall review the mechanisms and processes established under clause 6.2.1, including the baseline referred to in clause 6.2.2(b), at least once every 12 months, or as often as required based on the evolving cyber threat landscape, to ensure that the mechanisms and processes remain effective for their purposes. The first instance of this review is to be completed no later than 12 months from the time the mechanisms and processes are implemented.	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		MON-01
6.2.3	Monitoring and Detection	The CIIO shall review the mechanisms and processes established under clause 6.2.1, including the baseline referred to in clause 6.2.2(b), at least once every 12 months, or as often as required based on the evolving cyber threat landscape, to ensure that the mechanisms and processes remain effective for their purposes. The first instance of this review is to be completed no later than 12 months from the time the mechanisms and processes are implemented.	Functional	Intersects With	Alert Threshold Tuning	MON-07	Mechanisms exist to "tune" event monitoring technologies through analyzing communications traffic/event patterns and developing profiles representing common traffic patterns and/or events.	3		MON-01.13
6.2.4	Monitoring and Detection	The CIIO shall facilitate, if requested by the Commissioner, the deployment of CSA- supported threat detection systems across designated segments of the CIIO's network.	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
6.3.1	Threat Hunting	The CIIO shall conduct threat hunting for the CII to search for and identify cybersecurity threats to the CII at least once every 24 months. The first instance of threat hunting is to be completed no later than 12 months after the Compliance Date.	Functional	Intersects With	Threat Hunting	THR-13	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	8		THR-07
6.3.2	Threat Hunting	The CIIO shall include cybersecurity threats identified from threat hunting in cybersecurity risk assessments to ensure that the risks derived from the threats are assessed, mitigated, and tracked throughout the CII 's system development lifecycle.	Functional	Intersects With	Risk Assessment	RSK-13	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	5		RSK-04
6.3.2	Threat Hunting	The CIIO shall include cybersecurity threats identified from threat hunting in cybersecurity risk assessments to ensure that the risks derived from the threats are assessed, mitigated, and tracked throughout the CII 's system development lifecycle.	Functional	Intersects With	Threat Hunting	THR-13	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	5		THR-07
6.3.3	Threat Hunting	The CIIO shall analyse all threats identified from threat hunting to determine if there is or has been any cybersecurity incident in respect of the CII, and shall trigger the applicable incident reporting, response and recovery plans if there is or has been a cybersecurity incident.	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake;	3		IRO-02
6.3.3	Threat Hunting	The CIIO shall analyse all threats identified from threat hunting to determine if there is or has been any cybersecurity incident in respect of the CII, and shall trigger the applicable incident reporting, response and recovery plans if there is or has been a cybersecurity incident.	Functional	Intersects With	Threat Hunting	THR-13	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	5		THR-07
6.3.4	Threat Hunting	The CIIO shall, if requested by the Commissioner, submit a copy of the completed threat hunting report, to the Commissioner no later than 30 days upon receiving the request.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory	5		GOV-17
6.4.1	Cyber Threat Intelligence and Information Sharing	The CIIO shall establish and implement mechanisms and processes to obtain threat intelligence, and to process and analyse the threat intelligence for relevance and potential impact to the CII. Threat intelligence includes information on the current cybersecurity threat landscape; activities of threat actors; tactics, techniques and procedures of threat actors; and cybersecurity vulnerabilities.	Functional	Intersects With	Threat Intelligence Program	THR-02	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.	5		THR-01
6.4.1	Cyber Threat Intelligence and Information Sharing	The CIIO shall establish and implement mechanisms and processes to obtain threat intelligence, and to process and analyse the threat intelligence for relevance and potential impact to the CII. Threat intelligence includes information on the current cybersecurity threat landscape; activities of threat actors; tactics, techniques and procedures of threat actors; and cybersecurity vulnerabilities.	Functional	Intersects With	Threat Intelligence Feeds	THR-04	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		THR-03
6.4.2	Cyber Threat Intelligence and Information Sharing	The CIIO shall establish and implement mechanisms and processes to share information on cybersecurity threats and vulnerabilities, and on measures that can be taken in response to such threats and vulnerabilities, with the Commissioner for threat monitoring and analysis.	Functional	Intersects With	Sensitive / Regulated Data Sharing Decisions	DCH-08.1	Mechanisms exist to utilize a process to assist users in making information sharing decisions to ensure data is appropriately protected.	3		DCH-14
6.4.2	Cyber Threat Intelligence and Information Sharing	The CIIO shall establish and implement mechanisms and processes to share information on cybersecurity threats and vulnerabilities, and on measures that can be taken in response to such threats and vulnerabilities, with the Commissioner for threat monitoring and analysis.	Functional	Intersects With	Threat Intelligence Program	THR-02	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	5		THR-01
6.4.3	Cyber Threat Intelligence and Information Sharing	The CIIO shall put in place controls to mitigate cybersecurity threats and address vulnerabilities identified from threat intelligence.	Functional	Intersects With	Risk Remediation	RSK-17	Mechanisms exist to remediate risks to an acceptable level.	3		RSK-06
6.4.3	Cyber Threat Intelligence and Information Sharing	The CIIO shall put in place controls to mitigate cybersecurity threats and address vulnerabilities identified from threat intelligence.	Functional	Intersects With	Threat Intelligence Program	THR-02	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of	5		THR-01
7.1.1	Incident Management	The CIIO shall establish a Cybersecurity Incident Response Plan that sets out how a CIIO should respond to a cybersecurity incident. The CIIO shall ensure that the Plan establishes:	Functional	Intersects With	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	8		IRO-04
7.1.1	Incident Management	The CIIO shall establish a Cybersecurity Incident Response Plan that sets out how a CIIO should respond to a cybersecurity incident. The CIIO shall ensure that the Plan establishes:	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-11	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5		IRO-07
7.1.1(a)	Incident Management	A Cybersecurity Incident Response Team ("CIRT") structure, including clearly defined roles and responsibilities of each team member and their contact details;	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-11	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	8		IRO-07
7.1.1(b)	Incident Management	An incident reporting structure which sets out how the CIIO will comply with its reporting obligations under the Act and any other laws and regulations that apply to the CII;	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	8		IRO-10
7.1.1(b)	Incident Management	An incident reporting structure which sets out how the CIIO will comply with its reporting obligations under the Act and any other laws and regulations that apply to the CII;	Functional	Intersects With	Serious Incident Reporting	IRO-16.3	Mechanisms exist to report any serious incident involving the organization's Technology Assets, Applications, Services and/or Data (TAASD) to relevant authorities in the locality where the incident occurred, in accordance with mandatory reporting: (1) Requirements; and	5		IRO-10.5
7.1.1(c)	Incident Management	Communication and coordination structures to ensure the timely escalation of cybersecurity incidents to the CIRT and to the senior management of the CIIO;	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and	5		IRO-02
7.1.1(d)	Incident Management	Thresholds and procedures to activate the incident response and CIRT;	Functional	Intersects With	Incident Classification & Prioritization	IRO-04	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5		IRO-02.4
7.1.1(e)	Incident Management	Engagement protocols with external parties for forensic or recovery services and law enforcement agencies, and their contact details;	Functional	Intersects With	Regulatory & Law Enforcement Contacts	IRO-15	Mechanisms exist to maintain incident response contacts with applicable regulatory and law enforcement agencies.	5		IRO-14
7.1.1(f)	Incident Management	A communication plan to communicate information relating to a cybersecurity incident to internal and external stakeholders;	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10
7.1.1(g)	Incident Management	Processes and procedures to contain a cybersecurity incident, investigate the cause and impact of the cybersecurity incident, and to restore the CII 's operations;	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and	8		IRO-02
7.1.1(h)	Incident Management	Processes and procedures to collect and preserve digital forensic evidence before initiating the recovery process, to support investigations; and	Functional	Intersects With	Chain of Custody & Forensics	IRO-13	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-	8		IRO-08
7.1.1(i)	Incident Management	A post-incident root cause analysis review process to identify and implement corrective measures to prevent a recurrence.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future	8		IRO-13

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
7.1.2	Incident Management	The CIIO shall ensure that the CIRT is trained and equipped with the resources to respond to cybersecurity incidents.	Functional	Intersects With	Incident Response Training	IRO-10	Mechanisms exist to train personnel in their incident response roles and responsibilities.	5		IRO-05
7.1.2	Incident Management	The CIIO shall ensure that the CIRT is trained and equipped with the resources to respond to cybersecurity incidents.	Functional	Intersects With	Integrated Security Incident Response Team (ISIRT)	IRO-11	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity and data protection incident response operations.	5		IRO-07
7.1.3	Incident Management	The CIIO shall establish procedures to reset the Kerberos Ticket Granting Ticket account for CII assets that use the Kerberos authentication protocol for the domain controller, and shall reset the Kerberos Ticket Granting Ticket account in the event that the CII domain controller is compromised.	Functional	Intersects With	Events Requiring Authenticator Change	IAC-14.1	Mechanisms exist to change authentication credentials: (1) At predefined intervals; and/or (2) Upon suspicion of credential compromise.	5		IAC-10.13
7.1.3	Incident Management	The CIIO shall establish procedures to reset the Kerberos Ticket Granting Ticket account for CII assets that use the Kerberos authentication protocol for the domain controller, and shall reset the Kerberos Ticket Granting Ticket account in the event that the CII domain controller is compromised.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	3		IRO-04
7.1.4	Incident Management	The CIIO shall establish and implement processes to identify, investigate and address the root causes that contributed to each cybersecurity incident, including any structural, behavioural, managerial, technical or systemic factors, so as to prevent recurrence of similar incidents. This shall include processes to identify, investigate and address:	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	8		IRO-13
7.1.4(a)	Incident Management	Gaps in the existing cybersecurity governance structure that may have led to ineffective cybersecurity risk management and oversight efforts;	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future	3		IRO-13
7.1.4(b)	Incident Management	Gaps in and failure to comply with policies, standards and procedures which may have contributed to the cybersecurity incident; and	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future	3		IRO-13
7.1.4(c)	Incident Management	Gaps in the audit process and the remediation of audit findings which may have contributed to the cybersecurity incident.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-14	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future	3		IRO-13
7.1.5	Incident Management	The CIIO shall communicate the Cybersecurity Incident Response Plan to all persons who use, operate and manage the CII, including external parties, and update these persons whenever there is a change to the Cybersecurity Incident Response Plan.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-08	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5		IRO-04
7.1.6	Incident Management	The CIIO shall review the Cybersecurity Incident Response Plan to ensure that it remains updated and relevant at least once every 12 months or as often as required. The first instance of this review to be completed no later than 12 months from the time the plan is established.	Functional	Intersects With	Incident Response Plan (IRP) Update	IRO-08.1	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	8		IRO-04.2
7.1.7	Incident Management	The CIIO shall also review the Cybersecurity Incident Response Plan when there are material changes to the CII cyber operating environment or incident response requirements.	Functional	Intersects With	Incident Response Plan (IRP) Update	IRO-08.1	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as	5		IRO-04.2
7.1.8	Incident Management	The CIIO shall, if requested by the Commissioner, submit a copy of the Cybersecurity Incident Response Plan, to the Commissioner no later than 30 days upon receiving the request.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory	5		GOV-17
7.2.1	Crisis Communication Plan	The CIIO shall establish a Crisis Communication Plan to respond to a crisis arising from a cybersecurity incident.	Functional	Intersects With	Recovery Operations Communications	BCD-06	Mechanisms exist to communicate the status of recovery activities and progress in restoring operational capabilities to designated internal and external stakeholders.	3		BCD-01.6
7.2.1	Crisis Communication Plan	The CIIO shall establish a Crisis Communication Plan to respond to a crisis arising from a cybersecurity incident.	Functional	Intersects With	Public Relations & Reputation Repair	IRO-12	Mechanisms exist to proactively manage public relations associated with incidents and employ appropriate measures to prevent further reputational damage and	5		IRO-16
7.2.2	Crisis Communication Plan	The CIIO shall ensure that the Crisis Communication Plan:	Functional	Intersects With	Public Relations & Reputation Repair	IRO-12	Mechanisms exist to proactively manage public relations associated with incidents and employ appropriate measures to prevent further reputational damage and develop plans to repair any damage to the organization's	5		IRO-16
7.2.2(a)	Crisis Communication Plan	Establishes a crisis communication team to be activated during a crisis;	Functional	Intersects With	Public Relations & Reputation Repair	IRO-12	Mechanisms exist to proactively manage public relations associated with incidents and employ appropriate measures to prevent further reputational damage and develop plans to repair any damage to the organization's	3		IRO-16
7.2.2(b)	Crisis Communication Plan	Identifies probable cybersecurity incident scenarios and corresponding courses of action;	Functional	Intersects With	Incident Classification & Prioritization	IRO-04	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	3		IRO-02.4
7.2.2(b)	Crisis Communication Plan	Identifies probable cybersecurity incident scenarios and corresponding courses of action;	Functional	Intersects With	Public Relations & Reputation Repair	IRO-12	Mechanisms exist to proactively manage public relations associated with incidents and employ appropriate measures to prevent further reputational damage and	3		IRO-16
7.2.2(c)	Crisis Communication Plan	Identifies target audiences and stakeholders for each type of cybersecurity incident scenario, which may include employees, customers, and the general public;	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	3		IRO-10
7.2.2(d)	Crisis Communication Plan	Identifies spokespersons and technical experts who will represent the organisation when addressing the media;	Functional	Intersects With	Public Relations & Reputation Repair	IRO-12	Mechanisms exist to proactively manage public relations associated with incidents and employ appropriate measures to prevent further reputational damage and develop plans to repair any damage to the organization's	5		IRO-16
7.2.2(e)	Crisis Communication Plan	Identifies primary and alternate modes of communication for dissemination of information to relevant target audiences and stakeholders;	Functional	Intersects With	Alternate Communications Channels	BCD-06.1	Mechanisms exist to maintain command and control capabilities via alternate communications channels and designating alternative decision makers if primary decision makers are unavailable during a designated crisis	5		BCD-10.4
7.2.2(f)	Crisis Communication Plan	Establishes communication and coordination structures between the crisis communication team, spokespersons, technical experts, and any other relevant persons to ensure coordinated and consistent responses during a crisis; and	Functional	Intersects With	Public Relations & Reputation Repair	IRO-12	Mechanisms exist to proactively manage public relations associated with incidents and employ appropriate measures to prevent further reputational damage and develop plans to repair any damage to the organization's	3		IRO-16
7.2.2(g)	Crisis Communication Plan	Provides for crisis communication training to ensure that employees are able to perform their assigned roles.	Functional	Intersects With	Incident Response Training	IRO-10	Mechanisms exist to train personnel in their incident response roles and responsibilities.	3		IRO-05
7.2.3	Crisis Communication Plan	The CIIO shall communicate the Crisis Communication Plan to all relevant persons, including the crisis communication team, the spokespersons and the technical experts, and update these persons whenever there is a change to the Crisis Communication Plan.	Functional	Intersects With	Public Relations & Reputation Repair	IRO-12	Mechanisms exist to proactively manage public relations associated with incidents and employ appropriate measures to prevent further reputational damage and develop plans to repair any damage to the organization's	3		IRO-16
7.2.4	Crisis Communication Plan	The CIIO shall review the Crisis Communication Plan at least once every 12 months or as often as required, to ensure that the Crisis Communication Plan remains effective. The first instance of this review is to be completed no later than 12 months from the time the Crisis Communication Plan is established.	Functional	Intersects With	Public Relations & Reputation Repair	IRO-12	Mechanisms exist to proactively manage public relations associated with incidents and employ appropriate measures to prevent further reputational damage and develop plans to repair any damage to the organization's reputation.	3		IRO-16
7.2.5	Crisis Communication Plan	The CIIO shall, if requested by the Commissioner, submit a copy of the Crisis Communication Plan, to the Commissioner no later than 30 days upon receiving the request.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory	5		GOV-17
7.3.1	Cybersecurity Exercise	The CIIO shall develop a cybersecurity exercise plan that outlines the purpose, objectives, desired outcomes, scope, scenario, participant roles, logistics, and evaluation process for an exercise, ensuring everyone understands how it will be conducted. The exercise plan shall include:	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	3		BCD-04
7.3.1	Cybersecurity Exercise	The CIIO shall develop a cybersecurity exercise plan that outlines the purpose, objectives, desired outcomes, scope, scenario, participant roles, logistics, and evaluation process for an exercise, ensuring everyone understands how it will be conducted. The exercise plan shall include:	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5		IRO-06
7.3.1(a)	Cybersecurity Exercise	the Master Scenario Events List, which is a chronological schedule of scenario events and injects that guides exercise play, drives participant actions, and ensures the exercise objectives are met; and	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	3		IRO-06
7.3.1(b)	Cybersecurity Exercise	the entire planning and exercise schedule, communication arrangements, ground rules, post-exercise review activities to capture lessons learned, drive improvements.	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	3		IRO-06
7.3.2	Cybersecurity Exercise	The CIIO shall, if requested by the Commissioner, submit a copy of the exercise plan for review, to the Commissioner no later than 30 days upon receiving the request.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory	5		GOV-17
7.3.3	Cybersecurity Exercise	The CIIO shall conduct scenario-based cybersecurity exercises to test and validate the effectiveness of the following plans based on the exercise purpose and objectives:	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5		IRO-06
7.3.3	Cybersecurity Exercise	The CIIO shall conduct scenario-based cybersecurity exercises to test and validate the effectiveness of the following plans based on the exercise purpose and objectives:	Functional	Intersects With	Incident Response Capabilities Testing Coordination with Related Plans	IRO-09.1	Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans.	5		IRO-06.1
7.3.3(a)	Cybersecurity Exercise	Crisis Management Plan for decision-making (led by the CEO or a member from the Senior Management team);	Functional	Intersects With	Incident Response Capabilities Testing Coordination with Related Plans	IRO-09.1	Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans.	3		IRO-06.1
7.3.3(b)	Cybersecurity Exercise	Cybersecurity Incident Response Plan (led by the CISO or a suitably qualified personnel);	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5		IRO-06

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
7.3.3(c)	Cybersecurity Exercise	Sectoral Heightened Alert Plan (led by the CISO or a suitably qualified personnel);	Functional	Intersects With	Incident Response Capabilities Testing Coordination with Related Plans	IRO-09.1	Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans.	3		IRO-06.1
7.3.3(d)	Cybersecurity Exercise	Business Continuity Plan (led by the CIO or a suitably qualified personnel);	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5		BCD-04
7.3.3(e)	Cybersecurity Exercise	Disaster Recovery Plan (led by the CIO or a suitably qualified personnel);	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5		BCD-04
7.3.3(f)	Cybersecurity Exercise	Internal and External Stakeholders Communication Plan (led by the Head of Communications or a suitably qualified personnel); and	Functional	Intersects With	Incident Response Capabilities Testing Coordination with Related Plans	IRO-09.1	Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans.	3		IRO-06.1
7.3.3(g)	Cybersecurity Exercise	Improvement Plan(s) from previous exercise reviews (led by the CISO or a suitably qualified personnel).	Functional	Intersects With	Continuous Incident Response Improvements	IRO-03	Mechanisms exist to use qualitative and quantitative data from incident response testing to: (1) Determine the effectiveness of incident response processes; (2) Continuously improve incident response processes; and	3		IRO-04.3
7.3.4	Cybersecurity Exercise	The CIIO shall conduct the scenario-based cybersecurity exercises referred in clause 7.3.3 at least once every 12 months. The first instance of such exercises is to be completed no later than 12 months after the Compliance Date.	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5		IRO-06
7.3.5	Cybersecurity Exercise	The CIIO shall develop exercise scenarios based on threat modelling methodologies (e.g., STRIDE) to identify possible attack pathways and assess their potential impact on the CII and or interconnected systems. These scenarios shall be designed to test and validate:	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5		IRO-06
7.3.5	Cybersecurity Exercise	The CIIO shall develop exercise scenarios based on threat modelling methodologies (e.g., STRIDE) to identify possible attack pathways and assess their potential impact on the CII and or interconnected systems. These scenarios shall be designed to test and validate:	Functional	Intersects With	Threat Analysis	THR-08	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats.	3		THR-10
7.3.5(a)	Cybersecurity Exercise	the effectiveness and timeliness of responses to threats and vulnerabilities identified through threat intelligence and risk assessments;	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	3		IRO-06
7.3.5(b)	Cybersecurity Exercise	incident coordination, communication, decision-making, and escalation with plans with CSA, relevant stakeholders, and external parties;	Functional	Intersects With	Incident Response Capabilities Testing Coordination with Related Plans	IRO-09.1	Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans.	3		IRO-06.1
7.3.5(c)	Cybersecurity Exercise	the ability to maintain continuous monitoring, detection, and situational awareness for additional cybersecurity threats and incidents throughout the incident response process; and	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	3		MON-01
7.3.5(d)	Cybersecurity Exercise	the adequacy of the CIIO's personnel, processes, technologies, resources and capabilities to respond to, manage, and recover from cybersecurity incidents.	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	3		IRO-06
7.3.6	Cybersecurity Exercise	The exercise scenarios shall include (i) CII systems, and (ii) interconnected systems, based on the exercise objectives and scope to ensure holistic evaluation of cybersecurity readiness.	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	3		IRO-06
7.3.7	Cybersecurity Exercise	Based on the exercise objectives and scope, the CIIO shall ensure that the relevant stakeholders from the following list of categories participate in the cybersecurity exercises:	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	3		IRO-06
7.3.7	Cybersecurity Exercise	Based on the exercise objectives and scope, the CIIO shall ensure that the relevant stakeholders from the following list of categories participate in the cybersecurity exercises:	Functional	Intersects With	Incident Response Training	IRO-10	Mechanisms exist to train personnel in their incident response roles and responsibilities.	3		IRO-05
7.3.7(a)	Cybersecurity Exercise	Crisis management team (where the senior management team is involved per 7.3.3);	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	3		IRO-06
7.3.7(b)	Cybersecurity Exercise	CIRT;	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	3		IRO-06
7.3.7(c)	Cybersecurity Exercise	Business operation staff;	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	3		IRO-06
7.3.7(d)	Cybersecurity Exercise	Crisis communication team; and	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	3		IRO-06
7.3.7(e)	Cybersecurity Exercise	External Parties	Functional	Intersects With	Incident Response Capabilities Testing	IRO-09	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	3		IRO-06
7.3.8	Cybersecurity Exercise	The CIIO shall, if requested by the Commissioner, submit a copy of the completed cybersecurity exercise report, along with the CIIO's post-exercise improvement plans, to the Commissioner no later than 30 days of receiving the request.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	5		GOV-17
7.3.9	Cybersecurity Exercise	In relation to cybersecurity exercises conducted by the Commissioner under section 16 of the Act, the CIIO shall comply with any request by the Commissioner to provide information relating to the CII or interconnected systems, including the plans listed in clause 7.3.3, for the purpose of planning and conducting such exercises.	Functional	Intersects With	Security, Compliance & Resilience Status Reporting	CPL-27	Mechanisms exist to submit status reporting of the organization's security, compliance and/or resilience program to applicable statutory and/or regulatory authorities, as required.	3		GOV-17
7.3.10	Cybersecurity Exercise	The CIIOs shall assign personnel responsible for the cybersecurity of the CII, to participate in technical cybersecurity exercises organised by CSA or its designated partners at least once every 12 months.	Functional	Intersects With	Practical Security Training Exercises	SAT-09	Mechanisms exist to include practical exercises in security, compliance and resilience training that reinforce training objectives.	5		SAT-03.1
8.1.1	Backup and Restoration Plan	The CIIO shall establish a backup and restoration plan to ensure that its CII assets can be recovered in the event of system disruption or data corruption.	Functional	Intersects With	Data Backups	BCD-24	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	8		BCD-11
8.1.2	Backup and Restoration Plan	The CIIO shall perform periodic backups at a frequency that is commensurate with the CIIO's operational requirements and ensure that the backups are completed successfully.	Functional	Intersects With	Data Backups	BCD-24	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	5		BCD-11
8.1.3	Backup and Restoration Plan	The CIIO shall ensure that backups are stored on devices that are not connected to any computer or to the internet and are separate from the corresponding CII assets, and are protected from unauthorised access, modification and deletion.	Functional	Intersects With	Resilient Data Backup Architecture	BCD-23	Mechanisms exist to maintain a secure, immutable backup architecture.	5		
8.1.3	Backup and Restoration Plan	The CIIO shall ensure that backups are stored on devices that are not connected to any computer or to the internet and are separate from the corresponding CII assets, and are protected from unauthorised access, modification and deletion.	Functional	Intersects With	Data Backup Access	BCD-30	Mechanisms exist to restrict access to data backups to those privileged users with assigned roles for data backup and recovery operations.	5		BCD-11.9
8.1.4	Backup and Restoration Plan	The CIIO shall test the restoration of the backups periodically to ensure that they can be restored when required. The frequency of the tests shall be commensurate with the cybersecurity risk profile of the CII.	Functional	Intersects With	Testing for Reliability & Integrity	BCD-32	Mechanisms exist to routinely test data backups to verify the reliability of the backup process, as well as the integrity and availability of the data.	8		BCD-11.1
8.1.5	Backup and Restoration Plan	The CIIO shall review the backup and restoration plan at least once every 12 months to ensure that the plan remains relevant. The first instance of this review is to be completed no later than 12 months from the time the plan is established.	Functional	Intersects With	Data Backups	BCD-24	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	5		BCD-11
8.2.1	Business Continuity Plan and Disaster Recovery Plan	The CIIO shall establish a Business Continuity Plan ("BCP") and a Disaster Recovery Plan ("DRP") to ensure continuous delivery of essential services, in the event of disruption due to a cybersecurity incident.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and	8		BCD-01
8.2.1	Business Continuity Plan and Disaster Recovery Plan	The CIIO shall establish a Business Continuity Plan ("BCP") and a Disaster Recovery Plan ("DRP") to ensure continuous delivery of essential services, in the event of disruption due to a cybersecurity incident.	Functional	Intersects With	Business Continuity & Disaster Recovery (BC/DR) Plans	BCD-04	Mechanisms exist for process owners to establish and maintain formal Business Continuity & Disaster Recovery (BC/DR) plans to ensure information is detailed enough, accurate and representative of current operations in order to sustain and/or restore operations under adverse	5		BCD-01.7
8.2.2	Business Continuity Plan and Disaster Recovery Plan	The CIIO shall ensure that the BCP and DRP include plans for addressing different cybersecurity threat scenarios.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and	5		BCD-01
8.2.2	Business Continuity Plan and Disaster Recovery Plan	The CIIO shall ensure that the BCP and DRP include plans for addressing different cybersecurity threat scenarios.	Functional	Intersects With	Contingency Planning Components	BCD-07.1	Mechanisms exist to identify components that potentially impact the organization's ability to execute contingency plans, including changes to: (1) Personnel roles; (2) Business processes (including the use of third-party services); (3) Deployed technologies; (4) Data repositories and/or data flows; and/or	3		BCD-06.1
8.2.3	Business Continuity Plan and Disaster Recovery Plan	The CIIO shall define the recovery time objective and recovery point objective in the BCP.	Functional	Intersects With	Recovery Time / Point Objectives (RTO / RPO)	BCD-04.1	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8		BCD-01.4

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
8.2.4	Business Continuity Plan and Disaster Recovery Plan	For CII assets that use the Kerberos authentication protocol for the domain controller, the CIIO shall exercise the recovery procedures for the compromise of the Kerberos Ticket Granting Ticket as part of the disaster recovery exercise.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-10	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	3		BCD-04
8.2.4	Business Continuity Plan and Disaster Recovery Plan	For CII assets that use the Kerberos authentication protocol for the domain controller, the CIIO shall exercise the recovery procedures for the compromise of the Kerberos Ticket Granting Ticket as part of the disaster recovery exercise.	Functional	Intersects With	Events Requiring Authenticator Change	IAC-14.1	Mechanisms exist to change authentication credentials: (1) At predefined intervals; and/or (2) Upon suspicion of credential compromise.	3		IAC-10.13
8.2.5	Business Continuity Plan and Disaster Recovery Plan	The CIIO shall review the BCP and DRP plans at least once every 12 months to ensure their continued effectiveness. The first instance of this review is to be completed no later than 12 months from the time the respective plan is established.	Functional	Intersects With	Business Continuity Management System (BCMS)	BCD-02	Mechanisms exist to operate a Business Continuity Management System (BCMS) to achieve resilient Technology Assets, Applications, Services and/or Data (TAASD) during: (1) Routine operations; and	5		BCD-01
9.1.1	Cybersecurity Awareness Programme	The CIIO shall establish and implement a cybersecurity awareness programme to educate and develop cybersecurity awareness for all persons who use, operate and manage the CII, including external parties, including to:	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	8		SAT-02
9.1.1(a)	Cybersecurity Awareness Programme	Promote awareness of relevant laws, regulations, codes of practice, policies, standards, guidelines and procedures;	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is	5		SAT-02
9.1.1(b)	Cybersecurity Awareness Programme	Provide regular and timely communication covering general cybersecurity awareness messages and prevailing cybersecurity threats, impacts and mitigations; and	Functional	Intersects With	Cyber Threat Environment Situational Awareness	SAT-06	Mechanisms exist to provide role-based security, compliance and resilience awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5		SAT-03.6
9.1.1(c)	Cybersecurity Awareness Programme	Positively shape individual behaviour and the security culture of the organisation.	Functional	Intersects With	Security, Compliance & Resilience-Minded Workforce	SAT-02	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5		SAT-01
9.1.2	Cybersecurity Awareness Programme	The CIIO shall measure the effectiveness of the cybersecurity awareness programme in achieving the purposes stated in clause 9.1.1 through means such as quizzes and surveys at least once every 12 months. The first instance of such measuring is to be completed no later than 12 months after the programme is implemented.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	5		SAT-02
9.1.2	Cybersecurity Awareness Programme	The CIIO shall measure the effectiveness of the cybersecurity awareness programme in achieving the purposes stated in clause 9.1.1 through means such as quizzes and surveys at least once every 12 months. The first instance of such measuring is to be completed no later than 12 months after the programme is implemented.	Functional	Intersects With	Training Feedback	SAT-11	Mechanisms exist to: (1) Monitor individual training results; and (2) Report findings to stakeholders.	3		SAT-04.1
9.1.3	Cybersecurity Awareness Programme	The CIIO shall review the cybersecurity awareness programme at least once every 12 months to ensure that the programme remains current and relevant. The first instance of this review is to be completed no later than 12 months from the time the programme is established.	Functional	Intersects With	Maintaining Workforce Development Relevancy	SAT-03	Mechanisms exist to periodically review security workforce development and awareness training to account for changes to: (1) Organizational policies, standards and procedures; (2) Assigned roles and responsibilities; (3) Relevant threats and risks; and	5		SAT-01.1
9.1.3	Cybersecurity Awareness Programme	The CIIO shall review the cybersecurity awareness programme at least once every 12 months to ensure that the programme remains current and relevant. The first instance of this review is to be completed no later than 12 months from the time the programme is established.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-04	Mechanisms exist to provide all employees and contractors appropriate security, compliance and resilience awareness education and training that is relevant for their job function.	3		SAT-02
9.2.1	Cybersecurity Training and Skills	The CIIO shall ensure that all employees that operate and manage the CII attain the cybersecurity competencies necessary to perform their roles effectively.	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	5		HRS-03.2
9.2.1	Cybersecurity Training and Skills	The CIIO shall ensure that all employees that operate and manage the CII attain the cybersecurity competencies necessary to perform their roles effectively.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-05	Mechanisms exist to provide role-based security, compliance and resilience-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and	5		SAT-03
9.2.2	Cybersecurity Training and Skills	The CIIO shall maintain records of training attended by employees, including external parties, who operate and manage the CII.	Functional	Intersects With	Security, Compliance & Resilience Training Records	SAT-10	Mechanisms exist to document, retain and monitor individual training activities, including: (1) Initial security, compliance and resilience awareness training; (2) Recurring awareness training; and (3) Technology Assets, Applications and/or Services	8		SAT-04
9.2.3	Cybersecurity Training and Skills	The CIIO shall ensure that external parties that operate and manage the CII have the necessary cybersecurity competencies to perform their roles effectively.	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	5		HRS-03.2
9.2.3	Cybersecurity Training and Skills	The CIIO shall ensure that external parties that operate and manage the CII have the necessary cybersecurity competencies to perform their roles effectively.	Functional	Intersects With	Third-Party Personnel	HRS-13	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party security, compliance and/or resilience roles and responsibilities.	3		HRS-10
9.2.4	Cybersecurity Training and Skills	The CIIO shall ensure that any person or group of persons tasked with conducting a cybersecurity risk assessment for a CII is supervised by an individual possessing industry-recognised certification, such as Certified in Risk and Information Systems Control (CRISC). Where the industry recognised certification cannot be obtained, the CIIO shall explain how the cybersecurity risk assessment will be adequately supervised.	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	5		HRS-03.2
9.2.5	Cybersecurity Training and Skills	The CIIO shall ensure that any person or group of persons tasked with conducting a cybersecurity audit for a CII is supervised by an individual possessing industry-recognised certification, such as Certified Information Systems Auditor (CISA). Where the industry recognised certification cannot be obtained, the CIIO shall explain the reasons how the cybersecurity audit will be adequately supervised.	Functional	Intersects With	Assessment Team Subject Matter Expertise	CPL-09	Mechanisms exist to ensure individuals performing audits and/or assessments have reasonable: (1) Professional qualifications to perform the audit and/or assessment; and (2) Subject matter expertise to perform review, interview and test activities for in-scope People, Processes, Technologies, Data and/or Facilities (PPTDF).	5		CPL-01.6
9.2.5	Cybersecurity Training and Skills	The CIIO shall ensure that any person or group of persons tasked with conducting a cybersecurity audit for a CII is supervised by an individual possessing industry-recognised certification, such as Certified Information Systems Auditor (CISA). Where the industry recognised certification cannot be obtained, the CIIO shall explain the reasons how the cybersecurity audit will be adequately supervised.	Functional	Intersects With	Competency Requirements for Security, Compliance & Resilience-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security, compliance and resilience-related positions are staffed by qualified individuals who have the necessary skill set.	3		HRS-03.2
10.1.1	Application of this Section	This section shall apply to CII which are OT systems ("OT CII") .	Functional	No Relationship	N/A	N/A	N/A	0		
10.1.2	Application of this Section	In this section, the following terms shall have the corresponding meaning "alert suppression" The act of dismissing a notification. "fail - safe" A feature or practice that is designed to handle failure that results in minimal or no harm to equipment, environment and people. "field controller" Industrial computer (e.g., Programmable Logic Controller (PLC), Remote Terminal Unit (RTU)) in an OT environment used to monitor and/or control physical processes. "interlock" Mechanism, process or function to prevent operation (e.g., start-up, stoppage, etc) from entering in an undesired state. "physical process" An action or activity denoted by any change of operation states, such as valve movement (open to close status), circuit breaker activated (close to open status) and motor rotation (low to high speed). "programme code" The programmable code (e.g., Supervisory Control and Data Acquisition (SCADA) / Distributed Control System (DCS) function script, ladder diagram, function block diagram, structured text) developed for an application that is used to monitor and control the CII. "register block" A temporary memory space that is used by the field controller to store or manipulate data. "Safety Instrumented Control systems that take a physical process to a safe state System" when in conditions that are or may become hazardous.	Functional	Intersects With	Standardized Terminology	GOV-03.2	Mechanisms exist to standardize technology and process terminology to reduce confusion amongst groups and departments.	5		SEA-02.1
10.2.1	OT Architecture and Security	The CIIO shall ensure that the OT CII is not connected to any enterprise network except where necessary for operating the CII and provided that the direction of data flows is restricted to only one- way from the OT CII to the enterprise network.	Functional	Intersects With	Operational Technology (OT)	EMB-06	Mechanisms exist to proactively manage the security, compliance and resilience risks associated with Operational Technology (OT).	5		EMB-03
10.2.1	OT Architecture and Security	The CIIO shall ensure that the OT CII is not connected to any enterprise network except where necessary for operating the CII and provided that the direction of data flows is restricted to only one- way from the OT CII to the enterprise network.	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		NET-03
10.2.1	OT Architecture and Security	The CIIO shall ensure that the OT CII is not connected to any enterprise network except where necessary for operating the CII and provided that the direction of data flows is restricted to only one- way from the OT CII to the enterprise network.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network resources.	5		NET-06
10.2.2	OT Architecture and Security	The CIIO shall monitor the data flows from the OT CII to any enterprise network for anomalies and trigger an alert for investigation when any anomaly is detected.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other	5		MON-16

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
10.2.2	OT Architecture and Security	The CIIO shall monitor the data flows from the OT CII to any enterprise network for anomalies and trigger an alert for investigation when any anomaly is detected.	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-22	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5		MON-01.3
10.2.3	OT Architecture and Security	The CIIO shall implement separate authentication mechanisms and account credentials for users of the OT CII network and any enterprise network. This is to prevent threat actors from using compromised credentials across different operating environments.	Functional	Intersects With	Account Separation Between Infrastructure Environments	IAC-08.7	Mechanisms exist to separate non-privileged accounts between infrastructure environments to reduce the risk that a compromise in one infrastructure environment laterally affects another infrastructure environment.	8		IAC-15.10
10.2.3	OT Architecture and Security	The CIIO shall implement separate authentication mechanisms and account credentials for users of the OT CII network and any enterprise network. This is to prevent threat actors from using compromised credentials across different operating environments.	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-32	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	3		IAC-02
10.2.4	OT Architecture and Security	The CIIO shall ensure that the OT CII has fail-safes to ensure the safety and reliability of operations in the event of a cybersecurity incident .	Functional	Intersects With	Safe Operations	EMB-23	Mechanisms exist to continuously validate autonomous systems that trigger an automatic state change when safe	5		EMB-19
10.2.4	OT Architecture and Security	The CIIO shall ensure that the OT CII has fail-safes to ensure the safety and reliability of operations in the event of a cybersecurity incident .	Functional	Intersects With	Fail Safe	SEA-16	Mechanisms exist to implement fail-safe procedures when failure conditions occur.	8		SEA-07.3
10.2.5	OT Architecture and Security	The CIIO shall identify physical processes controlled by the OT CII and shall, to the extent possible, perform the following for each process:	Functional	Intersects With	Operational Technology (OT)	EMB-06	Mechanisms exist to proactively manage the security, compliance and resilience risks associated with	5		EMB-03
10.2.5(a)	OT Architecture and Security	Establish a baseline tolerance level for the operation time taken by the physical processes;	Functional	Intersects With	Operational Technology (OT)	EMB-06	Mechanisms exist to proactively manage the security, compliance and resilience risks associated with Operational Technology (OT).	3		EMB-03
10.2.5(a)	OT Architecture and Security	Establish a baseline tolerance level for the operation time taken by the physical processes;	Functional	Intersects With	Behavioral Baselining	THR-09	Automated mechanisms exist to establish behavioral baselines that capture information about user and entity	3		THR-11
10.2.5(b)	OT Architecture and Security	Monitor the duration of physical processes for deviations from the baseline tolerance level; and	Functional	Intersects With	Embedded Technology Configuration Monitoring	EMB-08	Mechanisms exist to generate log entries on embedded devices when configuration changes or attempts to access interfaces are detected.	3		EMB-05
10.2.5(b)	OT Architecture and Security	Monitor the duration of physical processes for deviations from the baseline tolerance level; and	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior	3		MON-16
10.2.5(c)	OT Architecture and Security	Ensure the field controller controlling the physical processes operate in a fail-safe state when deviations outside of the tolerance level occur and trigger an alert for investigation.	Functional	Intersects With	Safe Operations	EMB-23	Mechanisms exist to continuously validate autonomous systems that trigger an automatic state change when safe operation is no longer assured.	3		EMB-19
10.2.5(c)	OT Architecture and Security	Ensure the field controller controlling the physical processes operate in a fail-safe state when deviations outside of the tolerance level occur and trigger an alert for investigation.	Functional	Intersects With	Fail Safe	SEA-16	Mechanisms exist to implement fail-safe procedures when failure conditions occur.	5		SEA-07.3
10.2.6	OT Architecture and Security	The CIIO shall ensure that the Safety Instrumented System (SIS) is only connected to authorised field devices. This is to protect the SIS and its functions from being compromised in the event of a cybersecurity incident affecting other computers or computer systems.	Functional	Intersects With	Authorized Communications	EMB-17	Mechanisms exist to restrict embedded technologies to communicate only with authorized peers and service endpoints.	5		EMB-13
10.2.6	OT Architecture and Security	The CIIO shall ensure that the Safety Instrumented System (SIS) is only connected to authorised field devices. This is to protect the SIS and its functions from being compromised in the event of a cybersecurity incident affecting other computers or computer systems.	Functional	Intersects With	Safety Instrumented System (SIS)	EMB-25	Automated mechanisms exist to monitor and control hazardous processes to reduce the potential negative consequences of hazardous events.	8		
10.2.7	OT Architecture and Security	The CIIO shall periodically assess whether it is possible to replace CII assets (including legacy assets) with more secure versions, and make such replacements where possible to improve the cybersecurity of the CII.	Functional	Intersects With	Technology Lifecycle Management	AST-37	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	5		SEA-07.1
10.2.7	OT Architecture and Security	The CIIO shall periodically assess whether it is possible to replace CII assets (including legacy assets) with more secure versions, and make such replacements where possible to improve the cybersecurity of the CII.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5		TDA-17
10.3.1	Secure Coding	The CIIO shall verify the integrity of all embedded firmware of OT CII assets before they are used in the CII, and shall periodically verify the integrity of all embedded firmware in the OT CII.	Functional	Intersects With	Prevent Alterations	EMB-09	Mechanisms exist to protect embedded devices by preventing the unauthorized installation and execution of software.	3		EMB-06
10.3.1	Secure Coding	The CIIO shall verify the integrity of all embedded firmware of OT CII assets before they are used in the CII, and shall periodically verify the integrity of all embedded firmware in the OT CII.	Functional	Intersects With	Software / Firmware Integrity Verification	TDA-20.3	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware	5		TDA-14.1
10.3.2	Secure Coding	The CIIO shall verify the integrity of the programme codes in a field controller before use, and shall periodically verify the integrity of all programme codes in field controllers.	Functional	Intersects With	Prevent Alterations	EMB-09	Mechanisms exist to protect embedded devices by preventing the unauthorized installation and execution of software.	3		EMB-06
10.3.2	Secure Coding	The CIIO shall verify the integrity of the programme codes in a field controller before use, and shall periodically verify the integrity of all programme codes in field controllers.	Functional	Intersects With	Software / Firmware Integrity Verification	TDA-20.3	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware	5		TDA-14.1
10.3.3	Secure Coding	With regard to field controllers that are intended to have a fail-safe state, the CIIO shall identify and include interlocks in the field controller s' programme codes.	Functional	Intersects With	Safety Instrumented Function (SIF)	EMB-26	Automated mechanisms exist within a Safety Instrumented System (SIS) to execute predetermined actions upon detection of a potentially hazardous event.	5		
10.3.3	Secure Coding	With regard to field controllers that are intended to have a fail-safe state, the CIIO shall identify and include interlocks in the field controller s' programme codes.	Functional	Intersects With	Fail Safe	SEA-16	Mechanisms exist to implement fail-safe procedures when failure conditions occur.	3		SEA-07.3
10.3.4	Secure Coding	The CIIO shall establish mechanisms to validate the input values to the field controller to ensure that they are within a valid operational range.	Functional	Intersects With	Operational Technology (OT)	EMB-06	Mechanisms exist to proactively manage the security, compliance and resilience risks associated with	3		EMB-03
10.3.4	Secure Coding	The CIIO shall establish mechanisms to validate the input values to the field controller to ensure that they are within a valid operational range.	Functional	Intersects With	Input Data Validation	TDA-12	Mechanisms exist to check the validity of information inputs.	5		TDA-18
10.3.5	Secure Coding	The CIIO shall ensure that no unauthorised changes are made to the programme code or input values of a field controller.	Functional	Intersects With	Configuration Change Control	CHG-03	Mechanisms exist to govern the technical configuration change control processes.	5		CHG-02
10.3.5	Secure Coding	The CIIO shall ensure that no unauthorised changes are made to the programme code or input values of a field controller.	Functional	Intersects With	Prevent Alterations	EMB-09	Mechanisms exist to protect embedded devices by preventing the unauthorized installation and execution of	5		EMB-06
10.3.6	Secure Coding	The CIIO shall assign a separate and designated register block each for reading, writing, validating writes, calculation, and any other relevant function of the field controller, in order to facilitate data verification, prevent buffer overflows, prevent unauthorised writes and protect controller data.	Functional	Intersects With	Operational Technology (OT)	EMB-06	Mechanisms exist to proactively manage the security, compliance and resilience risks associated with Operational Technology (OT).	3		EMB-03
10.3.6	Secure Coding	The CIIO shall assign a separate and designated register block each for reading, writing, validating writes, calculation, and any other relevant function of the field controller, in order to facilitate data verification, prevent buffer overflows, prevent unauthorised writes and protect controller data.	Functional	Intersects With	Memory Protection	SEA-19	Mechanisms exist to implement security safeguards to protect system memory from unauthorized code execution.	3		SEA-10
10.3.7	Secure Coding	The CIIO shall identify programme codes in a field controller that function independently of other programme codes within the field controller, and modularise such programme codes to facilitate the detection of malicious codes.	Functional	Intersects With	Operational Technology (OT)	EMB-06	Mechanisms exist to proactively manage the security, compliance and resilience risks associated with Operational Technology (OT).	3		EMB-03
10.3.7	Secure Coding	The CIIO shall identify programme codes in a field controller that function independently of other programme codes within the field controller, and modularise such programme codes to facilitate the detection of malicious codes.	Functional	Intersects With	Developer Architecture & Design	TDA-04	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a design specification and security architecture that: (1) Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; (2) Accurately and completely describes the required security functionality and the allocation of security, compliance and resilience controls among physical and logical components; and (3) Expresses how individual security functions	3		TDA-05
10.4.1	Field Controllers	The CIIO shall establish mechanisms and processes to reduce and manage cybersecurity risks relating to connections between a field controller and any network or device, including:	Functional	Intersects With	Operational Technology (OT)	EMB-06	Mechanisms exist to proactively manage the security, compliance and resilience risks associated with Operational Technology (OT).	5		EMB-03
10.4.1	Field Controllers	The CIIO shall establish mechanisms and processes to reduce and manage cybersecurity risks relating to connections between a field controller and any network or device, including:	Functional	Intersects With	Network Security Controls (NSC)	NET-02	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	3		NET-01
10.4.1(a)	Field Controllers	Establishing a separate communication module when connecting the field controller to an external network or device, to prevent unauthorised access to the OT CII through the field controller;	Functional	Intersects With	Authorized Communications	EMB-17	Mechanisms exist to restrict embedded technologies to communicate only with authorized peers and service endpoints.	3		EMB-13
10.4.1(a)	Field Controllers	Establishing a separate communication module when connecting the field controller to an external network or device, to prevent unauthorised access to the OT CII through the field controller;	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.	3		NET-03
10.4.1(b)	Field Controllers	Implementing authentication processes for data transmission between the field controller and any network or device;	Functional	Intersects With	Identification & Authentication for Devices	IAC-34	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay	5		IAC-04
10.4.1(c)	Field Controllers	Preventing unauthorised data transmission, including unauthorised write functions, to ensure the safety and reliability of the operations;	Functional	Intersects With	Prevent Alterations	EMB-09	Mechanisms exist to protect embedded devices by preventing the unauthorized installation and execution of	3		EMB-06
10.4.1(c)	Field Controllers	Preventing unauthorised data transmission, including unauthorised write functions, to ensure the safety and reliability of the operations;	Functional	Intersects With	Restrict Communications	EMB-16	Mechanisms exist to require embedded technologies to initiate all communications and drop new, incoming	5		EMB-12
10.4.1(d)	Field Controllers	Preventing data transmission between the field controller and the network or device when the field controller is in a fault or error state, except where doing so would adversely affect the safety and reliability of operations; and	Functional	Intersects With	Safe Operations	EMB-23	Mechanisms exist to continuously validate autonomous systems that trigger an automatic state change when safe operation is no longer assured.	3		EMB-19

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
10.4.1(e)	Field Controllers	Enabling security features such as password-protection.	Functional	Intersects With	Operational Technology (OT)	EMB-06	Mechanisms exist to proactively manage the security, compliance and resilience risks associated with	3		EMB-03
10.4.1(e)	Field Controllers	Enabling security features such as password-protection.	Functional	Intersects With	Password-Based Authentication	IAC-15	Mechanisms exist to enforce complexity, length and lifespan considerations to ensure strong criteria for password-based authentication.	3		IAC-10.1
10.4.2	Field Controllers	The CIIO shall ensure that all alerts, errors and warnings from the field controllers are investigated in a timely manner.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Analysis & Triage	MON-05.2	Mechanisms exist to ensure event log and security-relevant telemetry reviews include analysis and triage practices that integrate with the organization's established incident response processes.	3		MON-17
10.4.2	Field Controllers	The CIIO shall ensure that all alerts, errors and warnings from the field controllers are investigated in a timely manner.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other	5		MON-16
10.4.3	Field Controllers	The CIIO shall establish mechanisms to monitor for alert suppression in the field controllers and trigger an alert for investigation when any unauthorised alert suppression is detected.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other	5		MON-16
10.4.4	Field Controllers	The CIIO shall establish baselines for normal day-to-day operational activities of field controllers, including baselines for cycle time, operational uptime, stop state, and memory usage, against which the CIIO is to monitor for deviations and anomalous activities, and trigger an alert for investigation when any deviation or anomaly is detected.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5		MON-16
10.4.4	Field Controllers	The CIIO shall establish baselines for normal day-to-day operational activities of field controllers, including baselines for cycle time, operational uptime, stop state, and memory usage, against which the CIIO is to monitor for deviations and anomalous activities, and trigger an alert for investigation when any deviation or anomaly is detected.	Functional	Intersects With	Behavioral Baselining	THR-09	Automated mechanisms exist to establish behavioral baselines that capture information about user and entity behavior to enable dynamic threat discovery.	8		THR-11
10.4.5	Field Controllers	The CIIO shall review the baselines referred to in clause 10.4.4 at least once every 12 months. The first instance of this review is to be completed no later than 12 months from the time the baseline is established.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other	3		MON-16
10.4.5	Field Controllers	The CIIO shall review the baselines referred to in clause 10.4.4 at least once every 12 months. The first instance of this review is to be completed no later than 12 months from the time the baseline is established.	Functional	Intersects With	Behavioral Baselining	THR-09	Automated mechanisms exist to establish behavioral baselines that capture information about user and entity behavior to enable dynamic threat discovery.	3		THR-11
11.1	Application of this Section	This section applies only to CII which CII assets include internet-facing Domain Name System (DNS) servers.	Functional	No Relationship	N/A	N/A	N/A	0		
11.2.1	Domain Name System Security Extension (DNSSEC)	The CIIO shall enable DNSSEC validation for its DNS resolvers, or implement any equivalent or better methods of validating the integrity of DNS records, to prevent DNS attacks such as DNS cache poisoning and DNS spoofing.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-13	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	3		NET-10
11.2.1	Domain Name System Security Extension (DNSSEC)	The CIIO shall enable DNSSEC validation for its DNS resolvers, or implement any equivalent or better methods of validating the integrity of DNS records, to prevent DNS attacks such as DNS cache poisoning and DNS spoofing.	Functional	Intersects With	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	NET-13.2	Mechanisms exist to perform data origin authentication and data integrity verification on the Domain Name Service (DNS) resolution responses received from authoritative sources when requested by client systems.	8		NET-10.2
11.2.2	Domain Name System Security Extension (DNSSEC)	The CIIO shall ensure that all domain names under its control and used in connection with the CII, including in the operation of the CII and in the delivery of services, are DNSSEC-signed on the corresponding DNS Authoritative Server for each domain name.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-13	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5		NET-10
12.1.1	Asset Management	With respect to the CIIO's obligations under clause 4.1.1, the CIIO shall establish mechanisms and processes to identify interconnected systems that are owned, managed or controlled by the CIIO regardless of proximity to the CII as long as there is a communication path to the CII. The inventory shall include the following:	Functional	Intersects With	Asset Inventories	AST-04	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	8		AST-02
12.1.1	Asset Management	With respect to the CIIO's obligations under clause 4.1.1, the CIIO shall establish mechanisms and processes to identify interconnected systems that are owned, managed or controlled by the CIIO regardless of proximity to the CII as long as there is a communication path to the CII. The inventory shall include the following:	Functional	Intersects With	Comprehensive Asset Inventory Management	AST-08	Mechanisms exist to maintain a dynamically updated inventory of Technology Assets, Applications, Services and/or Data (TAASD) that provides a highly contextualized understanding of every asset that is capable of providing operational visibility required to: (1) Detect anomalies; (2) Manage complex vulnerabilities; (3) Maintain compliance; and	5		
12.1.1(a)	Asset Management	Owner and/or operator of each interconnected system asset;	Functional	Intersects With	Technology Assets, Applications, Services and/or Data (TAASD) Ownership Assignment	AST-07.1	Mechanisms exist to ensure Technology Assets, Applications, Services and/or Data (TAASD) ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for	5		AST-03
12.1.1(b)	Asset Management	Name and description of each interconnected system asset;	Functional	Intersects With	Standardized Naming Convention	AST-03	Mechanisms exist to implement a scalable, standardized naming convention for Technology Assets, Applications, Services and/or Data (TAASD) that avoids asset naming conflicts.	3		AST-01.3
12.1.1(b)	Asset Management	Name and description of each interconnected system asset;	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use;	3		AST-02
12.1.1(c)	Asset Management	Description of critical functions of each interconnected system asset;	Functional	Intersects With	Identify Critical Assets	AST-05	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business	5		BCD-02
12.1.1(d)	Asset Management	Key person(s) responsible for the cybersecurity of each interconnected system asset;	Functional	Intersects With	Accountability Information	AST-07.2	Mechanisms exist to formally document the name, position and/or role of individuals responsible/accountable for administering assets as part	5		AST-03.1
12.1.1(e)	Asset Management	The dependencies of each interconnected system asset and the connections between each interconnected system asset and any systems or networks (whether internal or external to the interconnected system);	Functional	Intersects With	Asset-Service Dependencies	AST-06	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS) that support more than one critical business function.	5		AST-01.1
12.1.1(e)	Asset Management	The dependencies of each interconnected system asset and the connections between each interconnected system asset and any systems or networks (whether internal or external to the interconnected system);	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and	3		AST-04
12.1.1(f)	Asset Management	Physical location of each interconnected system asset;	Functional	Intersects With	Asset Inventories	AST-04	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	3		AST-02
12.1.1(g)	Asset Management	Outsourced service providers used to support each interconnected system asset;	Functional	Intersects With	Third-Party Inventories	TPM-08	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5		TPM-01.1
12.1.1(h)	Asset Management	Cloud services used to support each interconnected system asset; and	Functional	Intersects With	Asset Inventories	AST-04	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	3		AST-02

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
12.1.1(h)	Asset Management	Cloud services used to support each interconnected system asset; and	Functional	Intersects With	Cloud Services	CLD-02	Mechanisms exist to facilitate the implementation of cloud management controls to ensure cloud instances are secure and in-line with industry practices.	3		CLD-01
12.1.1(i)	Asset Management	Description of the internet links supporting the interconnected system, including information on the distributed denial-of-service (DDoS) attack mitigation measures in place for these internet links.	Functional	Intersects With	Asset Inventories	AST-04	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use;	3		AST-02
12.1.1(i)	Asset Management	Description of the internet links supporting the interconnected system, including information on the distributed denial-of-service (DDoS) attack mitigation measures in place for these internet links.	Functional	Intersects With	Denial of Service (DoS) Protection	NET-21	Automated mechanisms exist to protect against or limit the effects of denial of service attacks.	5		NET-02.1
12.1.2	Asset Management	The CIIO shall maintain an accurate CII network topology diagram with the interconnected systems identified and the interfaces and connectivity between the network devices and segments.	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-17	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and	8		AST-04
12.2.1	Account Management	The CIIO shall grant to each account only the minimum privileges necessary for its assigned functions across the interconnected systems.	Functional	Intersects With	Least Privilege	IAC-30	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.	8		IAC-21
12.2.2	Account Management	The CIIO shall delete or disable any account that is no longer necessary or is inactive to prevent unauthorised access to the interconnected systems.	Functional	Intersects With	Disable Inactive Accounts	IAC-08.4	Automated mechanisms exist to disable inactive accounts after an organization-defined time period.	8		IAC-15.3
12.2.3	Account Management	The CIIO shall perform a review of all accounts (e.g. privileged, user and application accounts) that have access to the interconnected systems. The review is to evaluate the validity of accounts and to ensure that privileges assigned to each account are up-to-date and required to support operational purposes.	Functional	Intersects With	Account Management	IAC-08	Mechanisms exist to: (1) Define authorized system account types; (2) Define prohibited system account types; and (3) Proactively govern individual, group, system, service, application, guest and temporary accounts.	3		IAC-15
12.2.3	Account Management	The CIIO shall perform a review of all accounts (e.g. privileged, user and application accounts) that have access to the interconnected systems. The review is to evaluate the validity of accounts and to ensure that privileges assigned to each account are up-to-date and required to support operational purposes.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	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		IAC-17
12.2.4	Account Management	The CIIO shall perform this review at least once every 12 months. The first instance of this review is to be completed no later than 12 months after the Compliance Date.	Functional	Intersects With	Periodic Review of Individual & Service Account Privileges	IAC-12	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.	3		IAC-17
12.3.1	Privileged Account Management	The CIIO shall implement multi-factor authentication where privileged accounts are used to access interconnected systems and where access is to be escalated to the level of privileged access (e.g., where the user seeks to obtain additional permissions on a system or network after an initial log-in).	Functional	Intersects With	Multi-Factor Authentication (MFA) For Network Access to Privileged Accounts	IAC-37.5	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for privileged accounts.	5		IAC-06.1
12.3.1	Privileged Account Management	The CIIO shall implement multi-factor authentication where privileged accounts are used to access interconnected systems and where access is to be escalated to the level of privileged access (e.g., where the user seeks to obtain additional permissions on a system or network after an initial log-in).	Functional	Intersects With	Multi-Factor Authentication (MFA) For Local Access to Privileged Accounts	IAC-37.7	Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts.	5		IAC-06.3
12.3.2	Privileged Account Management	The CIIO shall prohibit the sharing of privileged account(s) used by network and system administrators, and any other personnel with privileged access, across interconnected systems and establish processes to detect and remediate instances of account sharing.	Functional	Intersects With	Restrictions on Shared Groups / Accounts	IAC-21	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	3		IAC-15.5
12.3.2	Privileged Account Management	The CIIO shall prohibit the sharing of privileged account(s) used by network and system administrators, and any other personnel with privileged access, across interconnected systems and establish processes to detect and remediate instances of account sharing.	Functional	Intersects With	Credential Sharing	IAC-23	Mechanisms exist to prevent the sharing of generic IDs, passwords or other generic authentication methods.	5		IAC-19
12.3.3	Privileged Account Management	The CIIO shall restrict the use of "break glass" account(s) for administrative use during emergency where the normal administrative access is unavailable. Access to such account(s) shall be protected with access controls (e.g. "break glass" account password management process), logging and post-use review to ensure accountability.	Functional	Intersects With	Emergency Accounts	IAC-11	Mechanisms exist to establish and control "emergency access only" accounts.	8		IAC-15.9
12.3.3	Privileged Account Management	The CIIO shall restrict the use of "break glass" account(s) for administrative use during emergency where the normal administrative access is unavailable. Access to such account(s) shall be protected with access controls (e.g. "break glass" account password management process), logging and post-use review to ensure accountability.	Functional	Intersects With	Privileged Functions Logging	MON-14	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	3		MON-03.3
12.4.1	Network Segmentation	The CIIO shall segment the interconnected systems into different network segments based on their different security and risk levels.	Functional	Intersects With	Network Segmentation (macrosegmentation)	NET-06	Mechanisms exist to implement network segmentation within network architectures to isolate Technology Assets, Applications and/or Services (TAAS) from other network	8		NET-06
12.4.2	Network Segmentation	The CIIO shall implement firewalls at the boundaries between interconnected systems and between internet-facing assets and the enterprise environment, permitting only authorised traffic through defined firewall rules.	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		NET-03
12.4.2	Network Segmentation	The CIIO shall implement firewalls at the boundaries between interconnected systems and between internet-facing assets and the enterprise environment, permitting only authorised traffic through defined firewall rules.	Functional	Intersects With	Deny Traffic by Default & Allow Traffic by Exception	NET-04.1	Mechanisms exist to configure firewall and router configurations to deny network traffic by default and allow network traffic by exception (e.g., deny all and permit by exception).	5		NET-04.1
12.4.3	Network Segmentation	The CIIO shall monitor and block unauthorised outbound network connections from interconnected systems to secure network communications.	Functional	Intersects With	Inbound & Outbound Communications Traffic	MON-22	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5		MON-01.3
12.4.3	Network Segmentation	The CIIO shall monitor and block unauthorised outbound network connections from interconnected systems to secure network communications.	Functional	Intersects With	Prevent Unauthorized Exfiltration	NET-03.5	Automated mechanisms exist to prevent the unauthorized exfiltration of sensitive and/or regulated data across managed interfaces.	5		NET-03.5
12.5.1	System Hardening	The CIIO shall enable only ports, services or protocols that are necessary for the operations of the interconnected systems.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	8		CFG-03
12.5.2	System Hardening	The CIIO shall disable unused ports, services or protocols on internet-facing devices, such as routers, firewalls, and VPN gateways, that are not required for operations.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5		CFG-03
12.6.1	Patch Management	The CIIO shall establish and implement security patch management processes and apply security patches to interconnected systems in a timely manner to reduce cybersecurity vulnerabilities. Apply appropriate compensating controls to mitigate and reduce cybersecurity risks in cases where a security patch cannot be applied.	Functional	Intersects With	Compensating Countermeasures	RSK-18	Mechanisms exist to identify and implement one, or more, compensating controls to reduce risk and threat exposure when the primary means of implementing the security function is unavailable or compromised.	3		BCD-07 RSK-06.2
12.6.1	Patch Management	The CIIO shall establish and implement security patch management processes and apply security patches to interconnected systems in a timely manner to reduce cybersecurity vulnerabilities. Apply appropriate compensating controls to mitigate and reduce cybersecurity risks in cases where a security patch cannot be applied.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05
12.7.1	Monitoring and Detection	The CIIO shall establish and implement mechanisms and processes to review the activities (e.g. login and authentication events, configuration changes, remote access sessions) and traffic associated with the network management and monitoring servers across interconnected systems and investigate any anomalies detected that may indicate unauthorised access or suspicious behaviour. The review of the activities shall be conducted on a regular basis from the time the processes are implemented.	Functional	Intersects With	Event Log & Security-Relevant Telemetry Monitoring	MON-03	Mechanisms exist to review event logs and security-relevant telemetry on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5		MON-01.8
12.7.1	Monitoring and Detection	The CIIO shall establish and implement mechanisms and processes to review the activities (e.g. login and authentication events, configuration changes, remote access sessions) and traffic associated with the network management and monitoring servers across interconnected systems and investigate any anomalies detected that may indicate unauthorised access or suspicious behaviour. The review of the activities shall be conducted on a regular basis from the time the processes are implemented.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	3		MON-16
12.7.2	Monitoring and Detection	The CIIO shall establish and implement mechanisms and processes, and conduct the review of endpoint detection logs across interconnected systems including the identification of anomalous activities which do not trigger pre-configured alerts.	Functional	Intersects With	Endpoint Detection & Response (EDR)	END-09	Mechanisms exist to utilize Endpoint Detection & Response (EDR) capabilities to detect, investigate and respond to anomalous and/or malicious activity.	5		END-06.2

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
12.7.2	Monitoring and Detection	The CIIO shall establish and implement mechanisms and processes, and conduct the review of endpoint detection logs across interconnected systems including the identification of anomalous activities which do not trigger pre-configured alerts.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other	3		MON-16
12.7.3	Monitoring and Detection	The CIIO shall establish and implement mechanisms and processes to monitor virtualised environments used in interconnected systems including vCenter and ESXi hosts, for anomalous activities and trigger an alert for investigation when an anomaly is detected.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other	5		MON-16
12.7.3	Monitoring and Detection	The CIIO shall establish and implement mechanisms and processes to monitor virtualised environments used in interconnected systems including vCenter and ESXi hosts, for anomalous activities and trigger an alert for investigation when an anomaly is detected.	Functional	Intersects With	Virtualization Techniques	SEA-23	Mechanisms exist to utilize virtualization techniques to support the employment of a diversity of operating systems and applications.	3		SEA-13.1
12.7.4	Monitoring and Detection	The CIIO shall ensure that the virtualisation management infrastructure including vCenter Servers and ESXi hosts, run supported versions and are fully patched. Apply appropriate compensating controls to mitigate and reduce cybersecurity risks in cases where updates or patches cannot be applied.	Functional	Intersects With	Unsupported Technology Assets, Applications and/or Services (TAAS)	AST-39	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5		TDA-17
12.7.4	Monitoring and Detection	The CIIO shall ensure that the virtualisation management infrastructure including vCenter Servers and ESXi hosts, run supported versions and are fully patched. Apply appropriate compensating controls to mitigate and reduce cybersecurity risks in cases where updates or patches cannot be applied.	Functional	Intersects With	Software & Firmware Patching	VPM-08	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5		VPM-05
12.7.5	Monitoring and Detection	The CIIO shall establish and implement mechanisms and processes to report suspicious activities observed across the interconnected systems in accordance with the National Cybersecurity Incident Reporting Framework to CSA.	Functional	Intersects With	Incident Stakeholder Reporting	IRO-16	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5		IRO-10
12.7.6	Monitoring and Detection	The CIIO shall review the mechanisms and processes established under clauses 12.7.1, 12.7.2, 12.7.3 and 12.7.5 at least once every 12 months, or as often as required based on the evolving cyber threat landscape, to ensure that the mechanisms and processes remain effective for their purposes. The first instance of this review is to be completed no later than 12 months from the time the mechanisms and processes are implemented.	Functional	Intersects With	Continuous Monitoring	MON-02	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5		MON-01
A.1.1	Annex A - Security-by-Design	The CIIO should adopt the Security-by-Design Framework established by CSA to the extent that it applies to the system development lifecycle of a computer or computer system used by the organisation. Where there are parts of the Framework which do not apply to the system development lifecycle, the CIIO should document how and why these parts are not applicable.	Functional	Intersects With	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.	5		PRM-07
A.1.1	Annex A - Security-by-Design	The CIIO should adopt the Security-by-Design Framework established by CSA to the extent that it applies to the system development lifecycle of a computer or computer system used by the organisation. Where there are parts of the Framework which do not apply to the system development lifecycle, the CIIO should document how and why these parts are not applicable.	Functional	Intersects With	Security, Compliance & Resilience Aware Design	SEA-02	Mechanisms exist to formally incorporate the organization's secure architecture principles into engineering, product and model design requirements to ensure security, compliance and resilience are built in by default and by design.	5		SEA-01.5
A.2.1	Annex A - Cybersecurity Design Principles	The CIIO should adopt the defence-in-depth principle to ensure that the security architecture of a computer or computer system used by the organisation includes multiple layers of security controls to prevent single point of failure.	Functional	Intersects With	Defense-In-Depth (DiD) Architecture	SEA-06	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	8		NET-02 SEA-03
A.2.2	Annex A - Cybersecurity Design Principles	The CIIO should adopt the least privilege principle to ensure that accounts and users are granted the least extent of access necessary to perform their required functions.	Functional	Intersects With	Least Privilege	IAC-30	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.	8		IAC-21
A.2.3	Annex A - Cybersecurity Design Principles	The CIIO should adopt the principle of segregation of duties to ensure that duties and responsibilities for critical functions relating to a computer or computer system used by the organisation are divided among different persons.	Functional	Intersects With	Separation of Duties (SoD)	HRS-14	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	8		HRS-11
A.2.4	Annex A - Cybersecurity Design Principles	The CIIO should also adopt, to the extent possible, the following principles in relation to its people, process and technologies to reduce cybersecurity risks to a computer or computer system used by the organisation:	Functional	Intersects With	Secure Engineering Principles	SEA-05	Mechanisms exist to facilitate the implementation of industry-recognized security, compliance and resilience practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5		SEA-01
A.2.4(a)	Annex A - Cybersecurity Design Principles	The defence-by-diversity principle to reduce the number of potential attack vectors by having diversity throughout a computer or computer system used by the organisation, including diversity in technology, manufacturers and suppliers of assets, communication pathways, etc.; and	Functional	Intersects With	Heterogeneity	SEA-22	Mechanisms exist to utilize a diverse set of technologies for system components to reduce the impact of technical vulnerabilities from the same Original Equipment Manufacturer (OEM).	8		SEA-13
A.2.4(a)	Annex A - Cybersecurity Design Principles	The defence-by-diversity principle to reduce the number of potential attack vectors by having diversity throughout a computer or computer system used by the organisation, including diversity in technology, manufacturers and suppliers of assets, communication pathways, etc.; and	Functional	Intersects With	Supplier Diversity	TPM-06	Mechanisms exist to obtain security, compliance and resilience technologies from different suppliers to minimize supply chain risk.	3		TDA-03.1
A.2.4(b)	Annex A - Cybersecurity Design Principles	The zero-trust principle to ensure that each request for access to any computer or computer system used by the organisation is authenticated, authorised and validated for security configuration and posture before access is granted.	Functional	Intersects With	Zero Trust Architecture (ZTA)	NET-14	Mechanisms exist to treat all users and devices as potential threats and prevent access to data and resources until the users can be properly authenticated and their access authorized.	8		NET-01.1
A.3.1	Annex A - Wireless Communication	The CIIO should ensure that a computer or computer system used by the organisation is not connected to any wireless Local Area Network (LAN) except where necessary for authorised operations. Where any such connection is necessary, the CIIO should ensure that:	Functional	Intersects With	Disable Wireless Networking	CFG-04.18	Mechanisms exist to disable unnecessary wireless networking capabilities that are internally embedded within system components prior to issuance to end users.	5		NET-15.2
A.3.1	Annex A - Wireless Communication	The CIIO should ensure that a computer or computer system used by the organisation is not connected to any wireless Local Area Network (LAN) except where necessary for authorised operations. Where any such connection is necessary, the CIIO should ensure that:	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15
A.3.1(a)	Annex A - Wireless Communication	Only authorised wireless LAN is used;	Functional	Intersects With	Wireless Networking	NET-24	Mechanisms exist to control authorized wireless usage and monitor for unauthorized wireless access.	5		NET-15
A.3.1(b)	Annex A - Wireless Communication	The connection has strong encryption; and	Functional	Intersects With	Wireless Networking Authentication & Encryption	NET-24.1	Mechanisms exist to secure Wi-Fi (e.g., IEEE 802.11) and prevent unauthorized access by: (1) Authenticating devices trying to connect; and (2) Encrypting transmitted data.	8		NET-15.1
A.3.1(c)	Annex A - Wireless Communication	Only authorised devices are allowed to connect to the wireless LAN.	Functional	Intersects With	Authorized To Connect	AST-10.1	Mechanisms exist to maintain a list of Technology Asset, Application and/or Service (TAAS) that are authorized to connect to organizational Technology Assets, Applications, Services and/or Data (TAASD).	5		AST-01.5
A.3.1(c)	Annex A - Wireless Communication	Only authorised devices are allowed to connect to the wireless LAN.	Functional	Intersects With	Network Access Control (NAC)	NET-16	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, which is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	5		AST-02.5
A.4.1	Annex A - Vulnerability Assessment	The CIIO shall establish processes to identify and track cybersecurity vulnerabilities on IT systems used by the organisation.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02
A.4.2	Annex A - Vulnerability Assessment	The CIIO shall remediate all cybersecurity vulnerabilities in a timely manner, with priority given to vulnerabilities that pose a greater risk to the security or operations of the CII.	Functional	Intersects With	Vulnerability Ranking	VPM-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5		VPM-03
A.4.2	Annex A - Vulnerability Assessment	The CIIO shall remediate all cybersecurity vulnerabilities in a timely manner, with priority given to vulnerabilities that pose a greater risk to the security or operations of the CII.	Functional	Intersects With	Vulnerability Remediation Process	VPM-06	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5		VPM-02
A.4.3	Annex A - Vulnerability Assessment	The CIIO shall conduct a vulnerability assessment on an IT system used by the organisation at least once every 12 months and on an OT system used by the organisation system at least once every 24 months.	Functional	Intersects With	Vulnerability Scanning	VPM-12	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5		VPM-06
A.5.1	Annex A - Penetration Testing	The CIIO should conduct a penetration test on an IT system used by the organisation at least once every 12 months and on an OT system used by the organisation system at least once every 24 months.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		VPM-07
A.5.2	Annex A - Penetration Testing	The CIIO should conduct penetration tests on relevant assets after implementing any major system changes to computer or computer system used by the organisation. Major system changes include commissioning any new systems to be connected to the computer or computer system used by the organisation, implementing new application modules, system upgrades and technology refresh.	Functional	Intersects With	Penetration Testing	VPM-18	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5		VPM-07
A.5.3	Annex A - Penetration Testing	The CIIO should ensure that third-party penetration testing service providers and their penetration testers who are performing penetration tests on a computer or computer system used by the organisation possess industry-recognised accreditations and certifications respectively, for example CREST or equivalent accreditations and certifications.	Functional	Intersects With	Independent Penetration Agent or Team	VPM-19	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5		VPM-07.1

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes	Legacy SCF #
A.6.1	Annex A - Threat Hunting	The CIIO should conduct threat hunting for a computer or computer system used by the organisation to search for and identify cybersecurity threats to the systems at least once every 24 months. The first instance of threat hunting should be completed no later than 12 months after the Compliance Date.	Functional	Intersects With	Threat Hunting	THR-13	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	8		THR-07
A.6.2	Annex A - Threat Hunting	The CIIO should include cybersecurity threats identified from threat hunting in cybersecurity risk assessments to ensure that the risks derived from the threats are assessed, mitigated, and tracked throughout the the system development lifecycle of a computer or computer system used by the organisation.	Functional	Intersects With	Risk Assessment	RSK-13	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	5		RSK-04
A.6.2	Annex A - Threat Hunting	The CIIO should include cybersecurity threats identified from threat hunting in cybersecurity risk assessments to ensure that the risks derived from the threats are assessed, mitigated, and tracked throughout the the system development lifecycle of a computer or computer system used by the organisation.	Functional	Intersects With	Threat Hunting	THR-13	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	5		THR-07
A.6.3	Annex A - Threat Hunting	The CIIO should analyse all threats identified from threat hunting to determine if there is or has been any cybersecurity incident in respect of a computer or computer system used by the organisation, and should trigger the applicable incident reporting, response and recovery plans if there is or has been a cybersecurity incident.	Functional	Intersects With	Incident Handling	IRO-06	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis;	3		IRO-02
A.6.3	Annex A - Threat Hunting	The CIIO should analyse all threats identified from threat hunting to determine if there is or has been any cybersecurity incident in respect of a computer or computer system used by the organisation, and should trigger the applicable incident reporting, response and recovery plans if there is or has been a cybersecurity incident.	Functional	Intersects With	Threat Hunting	THR-13	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	5		THR-07
A.7.1	Annex A - Breach Attack Simulation	The CIIO should conduct Breach and Attack Simulation to continuously and automatically simulate real-world attack scenarios against the CIIO's defences to identify gaps.	Functional	Intersects With	Red Team Exercises	VPM-21	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	5		VPM-10
A.8.1	Annex A - Domain Name System	The CIIO should ensure that all domain names under its control and used in connection with any computer or computer system used by the organisation, including in the delivery of services, are DNSSEC-signed on the corresponding DNS Authoritative Server for each domain name.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-13	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5		NET-10
A.8.2	Annex A - Domain Name System	The CIIO should enable DNSSEC validation or implement any equivalent or better methods of validating the integrity of DNS records, for DNS resolver to prevent DNS attacks such as DNS cache poisoning and DNS spoofing.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-13	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	3		NET-10
A.8.2	Annex A - Domain Name System	The CIIO should enable DNSSEC validation or implement any equivalent or better methods of validating the integrity of DNS records, for DNS resolver to prevent DNS attacks such as DNS cache poisoning and DNS spoofing.	Functional	Intersects With	Secure Name / Address Resolution Service (Recursive or Caching Resolver)	NET-13.2	Mechanisms exist to perform data origin authentication and data integrity verification on the Domain Name Service (DNS) resolution responses received from authoritative sources when requested by client systems.	8		NET-10.2