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

Focal Document: Cyber Assessment Framework 4.0
Focal Document URL: https://www.ncsc.gov.uk/files/NCSC-Cyber-Assessment-Framework-4.0.pdf
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-eu-uk-caf-4-0.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
A1	Governance	The organisation has appropriate management policies, processes and procedures in place to govern its approach to the security of network and information systems.	Functional	Subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	10	
A1.a	Board Direction	You have effective organisational security management led at board level and articulated clearly in corresponding policies.	Functional	Subset of	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	10	
A1.b	Roles and Responsibilities	Your organisation has established roles and responsibilities for the security of network and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	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 cybersecurity and data protection program.	8	
A1.b	Roles and Responsibilities	Your organisation has established roles and responsibilities for the security of network and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.	Functional	Intersects With	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	5	
A1.b	Roles and Responsibilities	Your organisation has established roles and responsibilities for the security of network and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.	Functional	Intersects With	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	
A1.c	Decision-making	You have senior-level accountability for the security of network and information systems, and delegate decision-making authority appropriately and effectively. Risks to network and information systems related to the operation of your essential function(s) are considered in the context of other organisational risks.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	8	
A1.c	Decision-making	You have senior-level accountability for the security of network and information systems, and delegate decision-making authority appropriately and effectively. Risks to network and information systems related to the operation of your essential function(s) are considered in the context of other organisational risks.	Functional	Intersects With	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	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 cybersecurity and data protection program.	5	
A2	Risk Management	The organisation takes appropriate steps to identify, assess and understand security risks to network and information systems supporting the operation of essential functions. This includes an overall organisational approach to risk management.	Functional	Subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
A2.a	Risk Management Process	Your organisation has effective internal processes for managing risks to the security and resilience of network and information systems related to the operation of your essential function(s) and communicating associated activities.	Functional	Subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
A2.b	Understanding Threat	You understand the capabilities, methods and techniques of threat actors and what network and information systems they may compromise to adversely impact your essential function(s).	Functional	Subset of	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
A2.b	Understanding Threat	You understand the capabilities, methods and techniques of threat actors and what network and information systems they may compromise to adversely impact your essential function(s).	Functional	Intersects With	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	8	
A2.c	Assurance	You have gained confidence in the effectiveness of the security of your technology, people, and processes relevant to the operation of network and information systems supporting your essential function(s).	Functional	Intersects With	Assurance	GOV-19	Mechanisms exist to define the basis for confidence that implemented practices conform to applicable security, compliance and resilience controls, where the control implementation performs as intended.	8	
A2.c	Assurance	You have gained confidence in the effectiveness of the security of your technology, people, and processes relevant to the operation of network and information systems supporting your essential function(s).	Functional	Intersects With	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	8	
A3	Asset Management	Everything required to deliver, maintain or support network and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).	Functional	Subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
A3	Asset Management	Everything required to deliver, maintain or support network and information systems necessary for the operation of essential functions is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS), Applications and/or Services (TAAS) that support more than one critical business function.	8	
A3.a (point 1)	Asset Management	All assets relevant to the secure operation of network and information systems supporting your essential function(s) are identified and inventoried (at a suitable level of detail). The inventory is kept up-todate.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8	Sloppy writing. There is no clear control description for "Asset Management"
A3.a (point 2)	Asset Management	Dependencies on supporting infrastructure (e.g. power, cooling etc) are recognised and recorded.	Functional	Intersects With	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS), Applications and/or Services (TAAS) that support more than one critical business function.	8	Sloppy writing. There is no clear control description for "Asset Management"
A3.a (point 3)	Asset Management	You have prioritised your assets according to their importance to the operation of network and information systems supporting your essential function(s).	Functional	Intersects With	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	8	Sloppy writing. There is no clear control description for "Asset Management"
A3.a (point 4)	Asset Management	You have assigned responsibility for managing all assets, including physical assets, relevant to the operation of network and information systems supporting your essential function(s).	Functional	Intersects With	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	8	Sloppy writing. There is no clear control description for "Asset Management"
A3.a (point 4)	Asset Management	You have assigned responsibility for managing all assets, including physical assets, relevant to the operation of network and information systems supporting your essential function(s).	Functional	Intersects With	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	8	Sloppy writing. There is no clear control description for "Asset Management"
A3.a (point 5)	Asset Management	Assets relevant to network and information systems supporting your essential function(s) are managed with cyber security in mind throughout their lifecycle, from creation through to eventual decommissioning or disposal.	Functional	Subset of	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS).	10	Sloppy writing. There is no clear control description for "Asset Management"
A4	Supply Chain	The organisation understands and manages security risks to network and information systems supporting the operation of essential functions that arise as a result of dependencies on suppliers. This includes ensuring that appropriate measures are employed where third party services are used.	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	8	
A4	Supply Chain	The organisation understands and manages security risks to network and information systems supporting the operation of essential functions that arise as a result of dependencies on suppliers. This includes ensuring that appropriate measures are employed where third party services are used.	Functional	Subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
A4.a	Supply Chain	You understand and effectively manage the risks associated with suppliers to the security of network and information systems supporting the operation of your essential function(s).	Functional	Intersects With	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	8	
A4.b	Secure Software Development and Support	You actively maximise the use of secure and supported software, whether developed internally or sourced externally, within network and information systems supporting the operation of your essential function(s).	Functional	Subset of	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	10	
B1	Service Protection Policies, Processes and Procedures	The organisation defines, implements, communicates and enforces appropriate policies, processes and procedures that direct its overall approach to securing systems and data that support operation of essential functions.	Functional	Subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
B1.a	Policy, Process and Procedure Development	You have developed and continue to improve a set of cyber security and resilience policies, processes and procedures that manage and mitigate the risk of adverse impact to network and information systems supporting your essential function(s).	Functional	Subset of	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	10	
B1.b	Policy, Process and Procedure Implementation	You have successfully implemented your security policies, processes and procedures and can demonstrate the security benefits achieved.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	8	
B2	Identity and Access Control	The organisation understands, documents and manages access to network and information systems supporting the operation of essential functions. Users (or automated functions) that can access data or systems are appropriately verified, authenticated and authorised.	Functional	Subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
B2.a	Identity Verification, Authentication and Authorisation	You robustly verify, authenticate and authorise access to network and information systems supporting your essential function(s).	Functional	Intersects With	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	8	
B2.a	Identity Verification, Authentication and Authorisation	You robustly verify, authenticate and authorise access to network and information systems supporting your essential function(s).	Functional	Intersects With	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	8	
B2.b	Device Management	You fully know and have trust in the devices that are used to access your networks, information systems and data that support your essential function(s).	Functional	Intersects With	Identification & Authentication for Devices	IAC-04	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 resistant.	8	
B2.c	Privileged User Management	You closely manage privileged user access to network and information systems supporting your essential function(s).	Functional	Subset of	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS).	10	
B2.d	Identity and Access Management (IdAM)	You closely manage and maintain identity and access control for users, devices and systems accessing network and information systems supporting your essential function(s).	Functional	Subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
B3	Data Security	Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on essential functions. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the operation of essential functions. It also covers information that would assist a threat actor, such as design details of network and information systems	Functional	Subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
B3.a	Understanding Data	You have a good understanding of data important to the operation of network and information systems supporting your essential function(s), where it is stored, where it travels and how unavailability or unauthorised access, uncontrolled release, modification or deletion would adversely impact the essential function(s). This also applies to third parties storing or accessing data important to the operation of your essential function(s).	Functional	Intersects With	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	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) Document all sensitive/regulated data flows.	5	
B3.a	Understanding Data	You have a good understanding of data important to the operation of network and information systems supporting your essential function(s), where it is stored, where it travels and how unavailability or unauthorised access, uncontrolled release, modification or deletion would adversely impact the essential function(s). This also applies to third parties storing or accessing data important to the operation of your essential function(s).	Functional	Intersects With	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
B3.a	Understanding Data	You have a good understanding of data important to the operation of network and information systems supporting your essential function(s), where it is stored, where it travels and how unavailability or unauthorised access, uncontrolled release, modification or deletion would adversely impact the essential function(s). This also applies to third parties storing or accessing data important to the operation of your essential function(s).	Functional	Intersects With	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	5	
B3.a	Understanding Data	You have a good understanding of data important to the operation of network and information systems supporting your essential function(s), where it is stored, where it travels and how unavailability or unauthorised access, uncontrolled release, modification or deletion would adversely impact the essential function(s). This also applies to third parties storing or accessing data important to the operation of your essential function(s).	Functional	Intersects With	Data Access Mapping	DCH-14.3	Mechanisms exist to leverage data-specific Access Control Lists (ACL) or Interconnection Security Agreements (ISAs) to generate a logical map of the parties with whom sensitive/regulated data is shared.	5	
B3.a	Understanding Data	You have a good understanding of data important to the operation of network and information systems supporting your essential function(s), where it is stored, where it travels and how unavailability or unauthorised access, uncontrolled release, modification or deletion would adversely impact the essential function(s). This also applies to third parties storing or accessing data important to the operation of your essential function(s).	Functional	Intersects With	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	5	
B3.b	Data in Transit	You have protected the transit of data important to the operation of network and information systems supporting your essential function(s). This includes the transfer of data to third parties.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
B3.c	Stored Data	You have protected stored soft and hard copy data important to the operation of network and information systems supporting your essential function(s).	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	8	
B3.d	Mobile Data	You have protected data important to the operation of network and information systems supporting your essential function(s) on mobile devices (e.g. smartphones, tablets and laptops).	Functional	Subset of	Enterprise Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Enterprise Device Management (EDM) controls.	10	
B3.d	Mobile Data	You have protected data important to the operation of network and information systems supporting your essential function(s) on mobile devices (e.g. smartphones, tablets and laptops).	Functional	Subset of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
B3.e	Media / Equipment Sanitisation	Before reuse and / or disposal you appropriately sanitise devices, equipment and removable media holding data important to the operation of network and information systems supporting your essential function(s)	Functional	Intersects With	System Media Sanitization	DCH-09	Mechanisms exist to sanitize system media with the strength and integrity commensurate with the classification or sensitivity of the information prior to disposal, release out of organizational control or release for reuse.	8	
B4	System Security	Network and information systems and technology critical for the operation of essential functions are protected from cyber attack. An organisational understanding of risk to essential functions informs the use of robust and reliable protective security measures to effectively limit opportunities for threat actors to compromise networks and systems.	Functional	Subset of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
B4	System Security	Network and information systems and technology critical for the operation of essential functions are protected from cyber attack. An organisational understanding of risk to essential functions informs the use of robust and reliable protective security measures to effectively limit opportunities for threat actors to compromise networks and systems.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	8	
B4.a	Secure by Design	You design security into network and information systems that support the operation of your essential function(s). You minimise their attack surface and ensure that the operation of your essential function(s) should not be impacted by the exploitation of any single vulnerability.	Functional	Intersects With	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each system, application and/or service under their control.	8	
B4.a	Secure by Design	You design security into network and information systems that support the operation of your essential function(s). You minimise their attack surface and ensure that the operation of your essential function(s) should not be impacted by the exploitation of any single vulnerability.	Functional	Intersects With	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity and data protection controls for each system, application and/or service under their control.	8	
B4.a	Secure by Design	You design security into network and information systems that support the operation of your essential function(s). You minimise their attack surface and ensure that the operation of your essential function(s) should not be impacted by the exploitation of any single vulnerability.	Functional	Intersects With	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required cybersecurity and data protection controls for each system, application and/or service under their control.	8	
B4.a	Secure by Design	You design security into network and information systems that support the operation of your essential function(s). You minimise their attack surface and ensure that the operation of your essential function(s) should not be impacted by the exploitation of any single vulnerability.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
B4.b	Secure Configuration	You securely configure network and information systems that support the operation of your essential function(s).	Functional	Subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	10	
B4.c	Secure Management	You manage your organisation's network and information systems that support the operation of your essential function(s) to enable and maintain security.	Functional	Subset of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
B4.d	Vulnerability Management	You manage known vulnerabilities in network and information systems to prevent adverse impact on your essential function(s).	Functional	Subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
B5	Resilient Networks and Systems	The organisation builds resilience against cyber attack and system failure into the design, implementation, operation and management of systems that support the operation of your essential function(s).	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure cybersecurity and data protection controls are designed and implemented to provide resistance to: (1) Unintentional errors (by users or software); and (2) Intentional attack or circumvention.	8	
B5.a	Resilience Preparation	You are prepared to restore the operation of your essential function(s) following adverse impact to network and information systems	Functional	Subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
B5.b	Design for Resilience	You design network and information systems supporting your essential function(s) to be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated.	Functional	Intersects With	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	8	
B5.b	Design for Resilience	You design network and information systems supporting your essential function(s) to be resilient to cyber security incidents. Systems are appropriately segregated and resource limitations are mitigated.	Functional	Intersects With	Resilience Capabilities	SEA-01.3	Mechanisms exist to ensure cybersecurity and data protection controls are designed and implemented to provide resistance to: (1) Unintentional errors (by users or software); and (2) Intentional attack or circumvention.	8	
B5.c	Backups	You hold accessible and secured current backups of data and information needed to recover operation of your essential function(s) following an adverse impact to network and information systems.	Functional	Intersects With	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8	
B6	Staff Awareness and Training	Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the operation of your essential function(s).	Functional	Intersects With	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	8	
B6.a	Cyber Security Culture	You develop and maintain a positive cyber security culture and a shared sense of responsibility	Functional	Subset of	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
B6.b	Cyber Security Training	The people who support the operation of network and information systems supporting your essential function(s) are appropriately trained in cyber security.	Functional	Intersects With	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	8	
C1	Security Monitoring	The organisation monitors the security status of network and information systems supporting the operation of essential function(s) in order to detect security events indicative of a security incident.	Functional	Subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
C1.a	Sources and Tools for Logging and Monitoring	The data sources and tools that you include in your logging and monitoring allow for timely identification of events which might adversely affect the security or resiliency of network and information system(s) supporting the operation of your essential function(s).	Functional	Intersects With	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	5	
C1.a	Sources and Tools for Logging and Monitoring	The data sources and tools that you include in your logging and monitoring allow for timely identification of events which might adversely affect the security or resiliency of network and information system(s) supporting the operation of your essential function(s).	Functional	Intersects With	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
C1.a	Sources and Tools for Logging and Monitoring	The data sources and tools that you include in your logging and monitoring allow for timely identification of events which might adversely affect the security or resiliency of network and information system(s) supporting the operation of your essential function(s).	Functional	Intersects With	Content of Event Logs	MON-03	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 event.	5	
C1.b	Securing Logs	You hold log data securely and grant appropriate user and system access only to accounts with a business need. Log data is held for a suitable retention period, after which it is deleted.	Functional	Intersects With	Protection of Event Logs	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	8	
C1.b	Securing Logs	You hold log data securely and grant appropriate user and system access only to accounts with a business need. Log data is held for a suitable retention period, after which it is deleted.	Functional	Intersects With	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	8	
C1.c	Generating Alerts	Evidence of potential security incidents contained in your monitoring data is reliably identified and where appropriate triggers alerts.	Functional	Subset of	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	10	
C1.d	Triage of Security Alerts	You contextualise alerts with knowledge of the threat and your systems, to identify security incidents as well as responding to all alerts appropriately.	Functional	Intersects With	Event Log Analysis & Triage	MON-17	Mechanisms exist to ensure event log reviews include analysis and triage practices that integrate with the organization's established incident response processes.	8	
C1.e	Personnel Skills for Monitoring and Detection	Monitoring and detection personnel skills and roles, including those outsourced, reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring and detection personnel have sufficient knowledge of network and information systems and the essential function(s) they need to protect.	Functional	Intersects With	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	8	
C1.f	Understanding User's and System's Behaviour, and Threat Intelligence (within Security Monitoring)	Threats to the operation of network and information systems, and corresponding user and system behaviour, are sufficiently understood. These are used to detect cyber security incidents	Functional	Intersects With	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	5	
C1.f	Understanding User's and System's Behaviour, and Threat Intelligence (within Security Monitoring)	Threats to the operation of network and information systems, and corresponding user and system behaviour, are sufficiently understood. These are used to detect cyber security incidents	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	
C1.f	Understanding User's and System's Behaviour, and Threat Intelligence (within Security Monitoring)	Threats to the operation of network and information systems, and corresponding user and system behaviour, are sufficiently understood. These are used to detect cyber security incidents	Functional	Intersects With	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5	
C2	Threat Hunting	The organisation proactively seeks to detect, within networks and information systems, adverse activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard security prevent / detect solutions (or when standard solutions are not deployable).	Functional	Subset of	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	10	Sloppy writing. There is no clear control description for "Asset Management"
C2.a (point 1)	Threat Hunting	You understand the resources required to perform threat hunting and these are deployed as part of business as usual.	Functional	Subset of	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	10	Sloppy writing. There is no clear control description for "Asset Management"
C2.a (point 2)	Threat Hunting	You deploy threat hunting resources at a frequency that matches the risks posed to network and information systems supporting your essential function(s).	Functional	Subset of	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	10	Sloppy writing. There is no clear control description for "Asset Management"
C2.a (point 3)	Threat Hunting	Your threat hunts follow pre-determined and documented methods (e.g. hypothesis driven, data driven, entity driven) designed to identify adverse activity not detected by automated detections.	Functional	Subset of	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	10	Sloppy writing. There is no clear control description for "Asset Management"
C2.a (point 4)	Threat Hunting	You turn threat hunts into automated detections and alerting where appropriate	Functional	Subset of	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	10	Sloppy writing. There is no clear control description for "Asset Management"
C2.a (point 5)	Threat Hunting	You routinely record details of previous threat hunts and post hunt activities. You use these to drive improvements in your threat hunting and security posture	Functional	Subset of	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	10	Sloppy writing. There is no clear control description for "Asset Management"
C2.a (point 6)	Threat Hunting	You have justified confidence in the effectiveness of your threat hunts and the threat hunting process is reviewed and updated to match the risks posed to network and information systems supporting your essential function(s).	Functional	Subset of	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	10	Sloppy writing. There is no clear control description for "Asset Management"
C2.a (point 7)	Threat Hunting	You leverage automation to improve threat hunts where appropriate (e.g. some stages of the threat hunting process are automated)	Functional	Subset of	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	10	Sloppy writing. There is no clear control description for "Asset Management"
C2.a (point 8)	Threat Hunting	Your threat hunts focus on the tactics, techniques and procedures (TTPs) of threats over atomic IoCs (e.g. hashes, IP addresses, domain names etc)	Functional	Subset of	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	10	Sloppy writing. There is no clear control description for "Asset Management"
D1	Response and Recovery Planning	There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential function(s) in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.	Functional	Subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	Sloppy writing. There is no clear control description for "Asset Management"

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
D1.a	Response Plan	You have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of network and information systems supporting the operation of your essential function(s) and covers a range of incident scenarios.	Functional	Subset of	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	
D1.b	Response and Recovery Capability	You have the capability to enact your incident response plan, including effective limitation of impact on the operation of your essential function(s). During an incident, you have access to timely information on which to base your response decisions.	Functional	Subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
D1.c	Testing and Exercising	Your organisation carries out exercises to test response plans, using past incidents that affected your (and other) organisation, and scenarios that draw on threat intelligence and your risk assessment.	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	8	
D2	Lessons Learned	When an incident occurs, steps are taken to understand its causes and to ensure remediating action is taken to protect against future incidents.	Functional	Subset of	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	10	
D2.a	Post Incident Analysis	When an incident occurs, your organisation takes steps to understand its causes, informing appropriate remediating action.	Functional	Subset of	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	10	
D2.b	Using Incidents to Drive Improvements	Your organisation uses lessons learned from incidents to improve your security measures.	Functional	Subset of	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	10	