NIST IR 8477-Based Set Theory Relationship Mapp
Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **UK - Ministry of Defence Standard 05-138 (2024) - L3**
Focal Document URL: https://www.gov.uk/government/publications/cyber-security-for-defence-suppliers-def-stan-05-138-issue-4
Published STRM URL: https://content.securecontrolsframework.com/strm/scf-strm-emea-gbr-def-stan-05-138-l3-2024.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
0001	Cyber Essentials	The Supplier shall have Cyber Essentials certification that covers the scope required for all aspects of the contract and commit to maintaining this for the duration of the contract.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
0002	Cyber Essentials Plus	The Supplier shall have Cyber Essentials Plus certification that covers the scope required for all aspects of the contract and commit to maintaining this for the duration of the contract.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
1100	Governance	The Supplier shall have appropriate management policies and processes in place to govern their approach to the security of the network and information systems supporting Functions and protection of Data.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
1100	Governance	The Supplier shall have appropriate management policies and processes in place to govern their approach to the security of the network and information systems supporting Functions and protection of Data.	Functional	Subset Of	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	10	
1101	Board Direction	The Supplier shall 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 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.	10	
1101	Board Direction	The Supplier shall have effective organisational security management led at board level and articulated clearly in corresponding policies.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
1101	Board Direction	The Supplier shall have effective organisational security management led at board level and articulated clearly in corresponding policies.	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 Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
1102	Roles and Responsibilities	The Supplier shall have established roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.	Functional	Intersects With	Assigned Security, Compliance & Resilience 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 Security, Compliance & Resilience Program (SCRP).	5	
1102	Roles and Responsibilities	The Supplier shall have established roles and responsibilities for the security of networks and information systems at all levels, with clear and well-understood channels for communicating and escalating risks.	Functional	Equal	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
1103	Decision-Making	The Supplier shall have senior-level accountability for the security of networks and information systems, and delegates decision-making authority appropriately and effectively. Risks to network and information systems that protect all Data are considered in the context of other organisational risks.	Functional	Subset Of	Steering Committee & Program Oversight	GOV-01.1	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.	10	
1103	Decision-Making	The Supplier shall have senior-level accountability for the security of networks and information systems, and delegates decision-making authority appropriately and effectively. Risks to network and information systems that protect all Data are considered in the context of other organisational risks.	Functional	Intersects With	Assigned Security, Compliance & Resilience 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 Security, Compliance & Resilience Program (SCRP).	5	
1103	Decision-Making	The Supplier shall have senior-level accountability for the security of networks and information systems, and delegates decision-making authority appropriately and effectively. Risks to network and information systems that protect all Data are considered in the context of other organisational 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 Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	5	
1103	Decision-Making	The Supplier shall have senior-level accountability for the security of networks and information systems, and delegates decision-making authority appropriately and effectively. Risks to network and information systems that protect all Data are considered in the context of other organisational risks.	Functional	Subset Of	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 Technology Assets, Applications, Services and/or Data (TAASD)-related risks.	10	
1200	Risk Management	The Supplier shall take appropriate steps to identify, assess, understand and remediate security risks to the network and information systems that protect all Data. 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	
1200	Risk Management	The Supplier shall take appropriate steps to identify, assess, understand and remediate security risks to the network and information systems that protect all Data. This includes an overall organisational approach to risk management.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
1200	Risk Management	The Supplier shall take appropriate steps to identify, assess, understand and remediate security risks to the network and information systems that protect all Data. This includes an overall organisational approach to risk management.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
1200	Risk Management	The Supplier shall take appropriate steps to identify, assess, understand and remediate security risks to the network and information systems that protect all Data. This includes an overall organisational approach to risk management.	Functional	Intersects With	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
1201	Risk Management Process	The Supplier shall have effective internal processes for managing risks (to the security of network and information systems that protect all Data) and communicating associated activities and solutions.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
1202	Peridically Assess Risk	The Supplier shall periodically assess the risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals, resulting from the operation of organisational systems and the associated processing, storage, or transmission of Data.	Functional	Intersects With	Steering Committee & Program Oversight	GOV-01.1	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	
1202	Peridically Assess Risk	The Supplier shall periodically assess the risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals, resulting from the operation of organisational systems and the associated processing, storage, or transmission of Data.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
1203	Network Diagrams	The Supplier shall create and maintain up to date network diagrams detailing the network boundaries, internal and external connection, and systems within the operational environment.	Functional	Subset Of	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.	10	
1204	Threat Intelligence Capabilities	The Supplier shall implement threat intelligence capabilities (internally or externally) as part of a risk assessment to guide and inform the development of organisational systems, security architectures, selection of security solutions, monitoring, threat hunting, system security alerts and advisories, response and recovery activities.	Functional	Subset Of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
1204	Threat Intelligence Capabilities	The Supplier shall implement threat intelligence capabilities (internally or externally) as part of a risk assessment to guide and inform the development of organisational systems, security architectures, selection of security solutions, monitoring, threat hunting, system security alerts and advisories, response and recovery activities.	Functional	Intersects With	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
1204	Threat Intelligence Capabilities	The Supplier shall implement threat intelligence capabilities (internally or externally) as part of a risk assessment to guide and inform the development of organisational systems, security architectures, selection of security solutions, monitoring, threat hunting, system security alerts and advisories, response and recovery activities.	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	
1204	Threat Intelligence Capabilities	The Supplier shall implement threat intelligence capabilities (internally or externally) as part of a risk assessment to guide and inform the development of organisational systems, security architectures, selection of security solutions, monitoring, threat hunting, system security alerts and advisories, response and recovery activities.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
1204	Threat Intelligence Capabilities	The Supplier shall implement threat intelligence capabilities (internally or externally) as part of a risk assessment to guide and inform the development of organisational systems, security architectures, selection of security solutions, monitoring, threat hunting, system security alerts and advisories, response and recovery activities.	Functional	Intersects With	Threat Intelligence Reporting	THR-03.1	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.	5	
1205	Assurance	The Supplier shall gain validation for the effectiveness of the security of their technology, people, and processes in support of its Functions and which store and/or process Data.	Functional	Subset Of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of security, compliance and resilience assessment and authorization controls.	10	
1205	Assurance	The Supplier shall gain validation for the effectiveness of the security of their technology, people, and processes in support of its Functions and which store and/or process Data.	Functional	Intersects With	Assessments	IAO-02	Mechanisms exist to formally assess the security, compliance and resilience controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
1205	Assurance	The Supplier shall gain validation for the effectiveness of the security of their technology, people, and processes in support of its Functions and which store and/or process Data.	Functional	Intersects With	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical security, compliance and resilience controls.	5	
1206	Internal Controls Assurance	The Supplier shall monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. Any identified deficiencies should be recorded, reported to leadership, and mitigated within agreed timeframes.	Functional	Intersects With	Security, Compliance & Resilience Controls Oversight	CPL-02	Mechanisms exist to provide a security, compliance and resilience controls oversight function that reports to the organization's executive leadership.	5	
1206	Internal Controls Assurance	The Supplier shall monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. Any identified deficiencies should be recorded, reported to leadership, and mitigated within agreed timeframes.	Functional	Intersects With	Periodic Audits	CPL-02.2	Mechanisms exist to conduct periodic audits of security, compliance and resilience controls to evaluate conformity with the organization's documented policies, standards and procedures.	5	
1206	Internal Controls Assurance	The Supplier shall monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. Any identified deficiencies should be recorded, reported to leadership, and mitigated within agreed timeframes.	Functional	Intersects With	Functional Review Of Security, Compliance & Resilience Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) for adherence to the organization's security, compliance and/or resilience policies and standards.	5	
1300	Asset Management	The Supplier shall reasonably ensure everything required to deliver, maintain or support networks and information systems that support delivery of all Functions which protect all Data are determined and understood. This includes 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	
1300	Asset Management	The Supplier shall reasonably ensure everything required to deliver, maintain or support networks and information systems that support delivery of all Functions which protect all Data are determined and understood. This includes people and systems, as well as any supporting infrastructure (such as power or cooling).	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
1301	Automated Asset Inventory Management	The Supplier shall employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of data, people, systems and supporting infrastructure used to support business Functions and protect Data.	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	

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
1301	Automated Asset Inventory Management	The Supplier shall employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of data, people, systems and supporting infrastructure used to support business Functions and protect Data.	Functional	Subset Of	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.	10	
1301	Automated Asset Inventory Management	The Supplier shall employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of data, people, systems and supporting infrastructure used to support business Functions and protect Data.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	5	
1400	Supply Chain	The Supplier shall understand and manage security risks to Functions and Data that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.	Functional	Subset Of	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.	10	
1400	Supply Chain	The Supplier shall understand and manage security risks to Functions and Data that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.	Functional	Intersects With	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5	
1400	Supply Chain	The Supplier shall understand and manage security risks to Functions and Data that arise as a result of dependencies on external 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	
1400	Supply Chain	The Supplier shall understand and manage security risks to Functions and Data that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.	Functional	Intersects With	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
1401	External Provider Trusted Relationships	The Supplier shall establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	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).	5	
1401	External Provider Trusted Relationships	The Supplier shall establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships.	Functional	Intersects With	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure applicable security, compliance and resilience requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
1500	Physical Access Controls	The Supplier shall, unless prohibited by applicable law, restrict and monitor all physical access to facilities where Data is stored or processed to its authorised Personnel by implementing industry standard physical access controls. Examples of such controls include but are not limited to: i) Swipe card technology ii) Monitored CCTV iii) Remotely monitored alarm systems iv) On-premise security guards v) Photographic access credentials vi) Visitor escort vii) Physical access logs viii) Authorised access lists. The Supplier shall review physical access logs regularly or in the event of a physical or cybersecurity incident.	Functional	Subset Of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
1500	Physical Access Controls	The Supplier shall, unless prohibited by applicable law, restrict and monitor all physical access to facilities where Data is stored or processed to its authorised Personnel by implementing industry standard physical access controls. Examples of such controls include but are not limited to: i) Swipe card technology ii) Monitored CCTV iii) Remotely monitored alarm systems iv) On-premise security guards v) Photographic access credentials vi) Visitor escort vii) Physical access logs viii) Authorised access lists. The Supplier shall review physical access logs regularly or in the event of a physical or cybersecurity incident.	Functional	Intersects With	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
1500	Physical Access Controls	The Supplier shall, unless prohibited by applicable law, restrict and monitor all physical access to facilities where Data is stored or processed to its authorised Personnel by implementing industry standard physical access controls. Examples of such controls include but are not limited to: i) Swipe card technology ii) Monitored CCTV iii) Remotely monitored alarm systems iv) On-premise security guards v) Photographic access credentials vi) Visitor escort vii) Physical access logs viii) Authorised access lists. The Supplier shall review physical access logs regularly or in the event of a physical or cybersecurity incident.	Functional	Intersects With	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
1500	Physical Access Controls	The Supplier shall, unless prohibited by applicable law, restrict and monitor all physical access to facilities where Data is stored or processed to its authorised Personnel by implementing industry standard physical access controls. Examples of such controls include but are not limited to: i) Swipe card technology ii) Monitored CCTV iii) Remotely monitored alarm systems iv) On-premise security guards v) Photographic access credentials vi) Visitor escort vii) Physical access logs viii) Authorised access lists. The Supplier shall review physical access logs regularly or in the event of a physical or cybersecurity incident.	Functional	Intersects With	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	5	
1500	Physical Access Controls	The Supplier shall, unless prohibited by applicable law, restrict and monitor all physical access to facilities where Data is stored or processed to its authorised Personnel by implementing industry standard physical access controls. Examples of such controls include but are not limited to: i) Swipe card technology ii) Monitored CCTV iii) Remotely monitored alarm systems iv) On-premise security guards v) Photographic access credentials vi) Visitor escort vii) Physical access logs viii) Authorised access lists. The Supplier shall review physical access logs regularly or in the event of a physical or cybersecurity incident.	Functional	Intersects With	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	
1500	Physical Access Controls	The Supplier shall, unless prohibited by applicable law, restrict and monitor all physical access to facilities where Data is stored or processed to its authorised Personnel by implementing industry standard physical access controls. Examples of such controls include but are not limited to: i) Swipe card technology ii) Monitored CCTV iii) Remotely monitored alarm systems iv) On-premise security guards v) Photographic access credentials vi) Visitor escort vii) Physical access logs viii) Authorised access lists. The Supplier shall review physical access logs regularly or in the event of a physical or cybersecurity incident.	Functional	Intersects With	Intrusion Alarms / Surveillance Equipment	PES-05.1	Physical access control mechanisms exist to monitor physical intrusion alarms and surveillance equipment.	5	
1501	Physical Access Device Management	The Supplier shall manage and maintain an inventory of all physical access devices used on their premises. The inventory should contain a unique identifier for the device regardless of the type (e.g. RFID card, access fob or door key) as well as the named individual who it is assigned to.	Functional	Intersects With	Physical Access Device Inventories	PES-19	Mechanisms exist to maintain an accurate inventory of all physical access devices (e.g., RFID cards, access fobs, door keys, etc.).	5	
1502	Physical Access Restrictions	The Supplier shall restrict physical access to sensitive areas within an organisation's premises to only those who are authorised to have access. The Supplier shall maintain and manage an inventory of those staff who have privileged physical access.	Functional	Intersects With	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	5	
1502	Physical Access Restrictions	The Supplier shall restrict physical access to sensitive areas within an organisation's premises to only those who are authorised to have access. The Supplier shall maintain and manage an inventory of those staff who have privileged physical access.	Functional	Intersects With	Access To Critical Systems	PES-03.4	Physical access control mechanisms exist to enforce physical access to critical systems or sensitive/regulated data, in addition to the physical access controls for the facility.	5	
1503	Visitor Access Management	The Supplier shall ensure the following controls are applied to all visitors visiting the organisation's premises: i) Visitor access and exit shall be logged ii) All visitors shall wear visitor ID badges at all times. Visitor badges should visually differ from employee badges iii) All visitors should be appropriately escorted at all times while on the premises iv) Visitor badges should be returned to the organisation at the end of the day.	Functional	Intersects With	Retain Access Records	IAC-01.1	Mechanisms exist to retain a record of personnel accountability to ensure there is a record of all access granted to an individual (system and application-wise), who provided the authorization, when the authorization was granted and when the access was last reviewed.	5	
1503	Visitor Access Management	The Supplier shall ensure the following controls are applied to all visitors visiting the organisation's premises: i) Visitor access and exit shall be logged ii) All visitors shall wear visitor ID badges at all times. Visitor badges should visually differ from employee badges iii) All visitors should be appropriately escorted at all times while on the premises iv) Visitor badges should be returned to the organisation at the end of the day.	Functional	Intersects With	Distinguish Visitors from On-Site Personnel	PES-06.1	Physical access control mechanisms exist to easily distinguish between onsite personnel and visitors, especially in areas where sensitive/regulated data is accessible.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
1503	Visitor Access Management	The Supplier shall ensure the following controls are applied to all visitors visiting the organisation's premises: i) Visitor access and exit shall be logged ii) All visitors shall wear visitor ID badges at all times. Visitor badges should visually differ from employee badges iii) All visitors should be appropriately escorted at all times while on the premises iv) Visitor badges should be returned to the organisation at the end of the day.	Functional	Intersects With	Identification Requirement	PES-06.2	Physical access control mechanisms exist to requires at least one(1) form of government-issued or organization-issued photo identification to authenticate individuals before they can gain access to the facility.	5	
1503	Visitor Access Management	The Supplier shall ensure the following controls are applied to all visitors visiting the organisation's premises: i) Visitor access and exit shall be logged ii) All visitors shall wear visitor ID badges at all times. Visitor badges should visually differ from employee badges iii) All visitors should be appropriately escorted at all times while on the premises iv) Visitor badges should be returned to the organisation at the end of the day.	Functional	Intersects With	Visitor Access Revocation	PES-06.6	Mechanisms exist to ensure visitor badges, or other issued identification, are surrendered before visitors leave the facility or are deactivated at a pre-determined time/date of expiration.	5	
2100	Resilience Policy and Process Development	The Supplier shall develop, enact and regularly review cyber security and resilience policies and processes to manage and mitigate the risk of adverse impact on Functions and protection of Data.	Functional	Subset Of	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	10	
2100	Resilience Policy and Process Development	The Supplier shall develop, enact and regularly review cyber security and resilience policies and processes to manage and mitigate the risk of adverse impact on Functions and protection of Data.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	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.	5	
2100	Resilience Policy and Process Development	The Supplier shall develop, enact and regularly review cyber security and resilience policies and processes to manage and mitigate the risk of adverse impact on Functions and protection of Data.	Functional	Subset Of	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	10	
2101	Policy and Process Implementation	The Supplier shall develop, enact and regularly review cyber security and resilience policies and processes to manage and mitigate the risk of adverse impact on Functions and protection of Data.	Functional	Intersects With	Publishing Security, Compliance & Resilience Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate policies, standards and procedures necessary for secure, compliant and resilient capabilities.	5	
2101	Policy and Process Implementation	The Supplier shall develop, enact and regularly review cyber security and resilience policies and processes to manage and mitigate the risk of adverse impact on Functions and protection of Data.	Functional	Intersects With	Periodic Review & Update of Security, Compliance & Resilience Program	GOV-03	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.	5	
2101	Policy and Process Implementation	The Supplier shall develop, enact and regularly review cyber security and resilience policies and processes to manage and mitigate the risk of adverse impact on Functions and protection of Data.	Functional	Intersects With	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
2200	Identity and Access Control	The Supplier shall understand, document and manage (i.e create, review and disable) access to networks, information systems, and removable storage media & devices supporting Functions and protection of Data. All accounts and identities, including users, system and 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	
2200	Identity and Access Control	The Supplier shall understand, document and manage (i.e create, review and disable) access to networks, information systems, and removable storage media & devices supporting Functions and protection of Data. All accounts and identities, including users, system and automated functions that can access Data or systems are appropriately verified, authenticated and authorised.	Functional	Subset Of	Authenticate, Authorize and Audit (AAA)	IAC-01.2	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).	10	
2200	Identity and Access Control	The Supplier shall understand, document and manage (i.e create, review and disable) access to networks, information systems, and removable storage media & devices supporting Functions and protection of Data. All accounts and identities, including users, system and automated functions that can access Data or systems are appropriately verified, authenticated and authorised.	Functional	Intersects With	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
2201	Access Control - Multi-Factor Authentication	The Supplier shall implement multi-factor authentication (MFA) mechanisms to control access to critical or sensitive systems, and organisational operations. Factors can include: i) Something you know (e.g. password/personal identification number (PIN)) ii) Something you have (e.g. cryptographic identification device, token) iii) Something you are (e.g. biometric).	Functional	Subset Of	Multi-Factor Authentication (MFA)	IAC-06	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/regulated data.	10	
2202	Device Management	The Supplier shall fully understand and trust the devices that are used to access the network and information systems that support Functions and process Data.	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	
2202	Device Management	The Supplier shall fully understand and trust the devices that are used to access the network and information systems that support Functions and process Data.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
2202	Device Management	The Supplier shall fully understand and trust the devices that are used to access the network and information systems that support Functions and process Data.	Functional	Intersects With	Approved Baseline Deviations	AST-02.4	Mechanisms exist to document and govern instances of approved deviations from established baseline configurations.	5	
2203	Privileged User Management	The Supplier shall closely manage privileged user access and actions to networks and information systems supporting Functions and that protect Data.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
2203	Privileged User Management	The Supplier shall closely manage privileged user access and actions to networks and information systems supporting Functions and that protect Data.	Functional	Subset Of	Privileged User Oversight	MON-01.15	Mechanisms exist to implement enhanced activity monitoring for privileged users.	10	
2204	Principle of Least Functionality	The Supplier shall ensure that all information systems are configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, such as ports, protocols, programmes and services that are not integral to the operation of that information system.	Functional	Subset Of	Secure 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	
2204	Principle of Least Functionality	The Supplier shall ensure that all information systems are configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, such as ports, protocols, programmes and services that are not integral to the operation of that information system.	Functional	Equal	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	10	
2205	Least Privilege	The Supplier shall closely manage all user accounts and employ the principle of least privilege to networks and information systems supporting all Functions and protecting all Data.	Functional	Equal	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	10	
2206	Least Privilege - Audit System	The Supplier shall limit access to systems' audit/security logging data and functionality to privileged user groups that have a confirmed requirement in accordance with the principle of least privilege.	Functional	Subset Of	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	10	
2206	Least Privilege - Audit System	The Supplier shall limit access to systems' audit/security logging data and functionality to privileged user groups that have a confirmed requirement in accordance with the principle of least privilege.	Functional	Intersects With	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
2207	Separation of Duties	The Supplier shall develop a policy and implement a separation of duties methodology for standard and privileged accounts which support Functions and protect Data.	Functional	Intersects With	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	
2208	Identity and Access Management (IdAM)	The Supplier shall closely manage and maintain identity and access control for users/admins, devices and systems accessing their networks and information systems supporting business Functions and protecting all Data.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
2209	Limit Access to Authorised Entities	The Supplier shall implement automated mechanisms to support the management of system accounts, including processes acting on behalf of authorised users.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	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	
2209	Limit Access to Authorised Entities	The Supplier shall implement automated mechanisms to support the management of system accounts, including processes acting on behalf of authorised users.	Functional	Intersects With	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
2210	Limit to Authorised Transactions	The Supplier shall issue, manage, verify, revoke, and audit identities and credentials to authorised transactions. users, and processes.	Functional	Subset Of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
2210	Limit to Authorised Transactions	The Supplier shall issue, manage, verify, revoke, and audit identities and credentials to authorised transactions. users, and processes.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	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	
2211	Secure First-Time Password Management	The Supplier shall employ secure practices for the secure storage, transmission, and management of first-time and one-time passwords. These practices include, but are not limited to: i) Secure storage of first-time password prior to use ii) Secure transmission of first-time and one-time passwords to their new user iii) Require first-time and one-time passwords are immediately changed after first logon.	Functional	Intersects With	Default Authenticators	IAC-10.8	Mechanisms exist to ensure default authenticators are changed as part of account creation or system installation.	8	
2212	Automated Password Management	The Supplier shall employ automated mechanisms for the generation, protection, storage, rotation, transmission, cryptographic protection and management of passwords for staff and systems.	Functional	Subset Of	Password Managers	IAC-10.11	Mechanisms exist to protect and store passwords via a password manager tool.	10	
2213	Automated Password Quality Check	The Supplier shall deploy technical controls to manage the quality of credentials across all identifiers. The technical controls should reflect industry standard requirements such as password length, complexity requirements (e.g. uppercase, lowercase, numbers and symbols), reuse history, prevent reuse of identifiers for a defined period, banned words and insecure pattern recognition (e.g. 1234), as appropriate.	Functional	Intersects With	Automated Support For Password Strength	IAC-10.4	Automated mechanisms exist to determine if password authenticators are sufficiently strong enough to satisfy organization-defined password length and complexity requirements.	8	
2214	Repeated Unsuccessful Logon Handling	The Supplier shall employ policies and processes to appropriately manage unsuccessful login attempts to standard and privileged accounts. The Supplier shall lock accounts after at most ten unsuccessful login attempts for a minimum of 15 minutes; the duration of which should increase between multiple account lockouts.	Functional	Intersects With	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	8	
2215	Replay-Resistant Authentication	The Supplier shall enforce technical control to protect against the capture of transmitted authentication or access control information and its subsequent retransmission i.e replay attacks.	Functional	Intersects With	Replay-Resistant Authentication	IAC-02.2	Automated mechanisms exist to employ replay-resistant authentication.	8	
2216	Privilege Failure Handling	The Supplier shall prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Functional	Equal	Prohibit Non-Privileged Users from Executing Privileged Functions	IAC-21.5	Mechanisms exist to prevent non-privileged users from executing privileged functions to include disabling, circumventing or altering implemented security safeguards / countermeasures.	10	
2216	Privilege Failure Handling	The Supplier shall prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Functional	Intersects With	Privileged Functions Logging	MON-03.3	Mechanisms exist to log and review the actions of users and/or services with elevated privileges.	5	
2217	Service Accounts	The Supplier shall inventory all generic, service and system accounts used on the network. Every account shall be owned by a single named individual who is responsible and accountable for the account and its usage.	Functional	Subset Of	User & Service Account Inventories	IAC-01.3	Mechanisms exist to maintain a current list of authorized users and service accounts.	10	
2218	System Users and Processes	The Supplier shall identify system users, processes acting on behalf of users, and devices.	Functional	Subset Of	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.	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	Notes
2218	System Users and Processes	The Supplier shall identify system users, processes acting on behalf of users, and devices.	Functional	Intersects With	Automated System Account Management (Directory Services)	IAC-15.1	Automated mechanisms exist to support the management of system accounts (e.g., directory services).	5	
2301	Understanding Data	The Supplier shall have a good understanding and classification of the data important to the operation of Functions and protection of Data, including where it is stored, where it travels, the application of protective markings to media. The Supplier shall understand how unauthorised access, modification or availability of data would adversely impact the organisation. This shall apply to data released to third parties including those important to the operation of Functions and protection of all Data.	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.	8	
2301	Understanding Data	The Supplier shall have a good understanding and classification of the data important to the operation of Functions and protection of Data, including where it is stored, where it travels, the application of protective markings to media. The Supplier shall understand how unauthorised access, modification or availability of data would adversely impact the organisation. This shall apply to data released to third parties including those important to the operation of Functions and protection of all Data.	Functional	Intersects With	Defining Access Authorizations for Sensitive / Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data.	5	
2301	Understanding Data	The Supplier shall have a good understanding and classification of the data important to the operation of Functions and protection of Data, including where it is stored, where it travels, the application of protective markings to media. The Supplier shall understand how unauthorised access, modification or availability of data would adversely impact the organisation. This shall apply to data released to third parties including those important to the operation of Functions and protection of all Data.	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	
2301	Understanding Data	The Supplier shall have a good understanding and classification of the data important to the operation of Functions and protection of Data, including where it is stored, where it travels, the application of protective markings to media. The Supplier shall understand how unauthorised access, modification or availability of data would adversely impact the organisation. This shall apply to data released to third parties including those important to the operation of Functions and protection of all Data.	Functional	Intersects With	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
2301	Understanding Data	The Supplier shall have a good understanding and classification of the data important to the operation of Functions and protection of Data, including where it is stored, where it travels, the application of protective markings to media. The Supplier shall understand how unauthorised access, modification or availability of data would adversely impact the organisation. This shall apply to data released to third parties including those important to the operation of Functions and protection of all Data.	Functional	Intersects With	Applied Security, Compliance and Resilience Controls Documentation	IAO-03	Mechanisms exist to generate authoritative documentation (e.g., System Security Plan (SSP)) that: (1) Identifies key architectural and implementation information on in-scope Technology Assets, Applications and/or Services (TAAS); (2) Reflects the current state of applied security, compliance and resilience controls on applicable People, Processes, Technologies, Data and/or Facilities (PPTDF) that are contained within the system boundary; and (3) Provides a historical record of applied security controls, including changes.	5	
2302	Data in Transit	The Supplier shall protect and control data in transit, including the use of encryption where appropriate, for data important to the operation of the Functions and all Data. 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.	5	
2302	Data in Transit	The Supplier shall protect and control data in transit, including the use of encryption where appropriate, for data important to the operation of the Functions and all Data. This includes the transfer of data to third parties.	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5	
2302	Data in Transit	The Supplier shall protect and control data in transit, including the use of encryption where appropriate, for data important to the operation of the Functions and all Data. This includes the transfer of data to third parties.	Functional	Intersects With	Encrypting Data In Storage Media	DCH-07.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	8	
2303	Management of Established Network Connections	The Supplier shall terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity	Functional	Intersects With	Network Connection Termination	NET-07	Mechanisms exist to terminate network connections at the end of a session or after an organization-defined time period of inactivity.	5	
2304	Wireless Network Access Controls	The Supplier shall ensure that the following controls apply to trusted organisational wireless networks: i) All users and devices must be authorised and authenticated prior to granting access to the network via the wireless network ii) The data transferred over the wireless network must be encrypted using WPA2 or above methodology.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
2304	Wireless Network Access Controls	The Supplier shall ensure that the following controls apply to trusted organisational wireless networks: i) All users and devices must be authorised and authenticated prior to granting access to the network via the wireless network ii) The data transferred over the wireless network must be encrypted using WPA2 or above methodology.	Functional	Intersects With	Authenticate, Authorize and Audit (AAA)	IAC-01.2	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	
2304	Wireless Network Access Controls	The Supplier shall ensure that the following controls apply to trusted organisational wireless networks: i) All users and devices must be authorised and authenticated prior to granting access to the network via the wireless network ii) The data transferred over the wireless network must be encrypted using WPA2 or above methodology.	Functional	Intersects With	Authentication & Encryption	NET-15.1	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	
2305	Remote Access - VPN (Virtual Private Network)	The Supplier shall ensure the following controls are enforced for staff to connect to organisational networks and systems using Remote Access technologies, for example VPN: i) Enable MFA prior to establishing a remote connection to the network ii) Encrypt all data transmitted over a VPN connection iii) Disable split-tunnelling to ensure all Data is only transmitted via organisation controlled channels.	Functional	Intersects With	Split Tunneling	CFG-03.4	Mechanisms exist to prevent split tunneling for remote devices unless the split tunnel is securely provisioned using organization-defined safeguards.	5	
2305	Remote Access - VPN (Virtual Private Network)	The Supplier shall ensure the following controls are enforced for staff to connect to organisational networks and systems using Remote Access technologies, for example VPN: i) Enable MFA prior to establishing a remote connection to the network ii) Encrypt all data transmitted over a VPN connection iii) Disable split-tunnelling to ensure all Data is only transmitted via organisation controlled channels.	Functional	Subset Of	Multi-Factor Authentication (MFA)	IAC-06	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/regulated data.	10	
2305	Remote Access - VPN (Virtual Private Network)	The Supplier shall ensure the following controls are enforced for staff to connect to organisational networks and systems using Remote Access technologies, for example VPN: i) Enable MFA prior to establishing a remote connection to the network ii) Encrypt all data transmitted over a VPN connection iii) Disable split-tunnelling to ensure all Data is only transmitted via organisation controlled channels.	Functional	Intersects With	Safeguarding Data Over Open Networks	NET-12	Cryptographic mechanisms exist to implement strong cryptography and security protocols to safeguard sensitive/regulated data during transmission over open, public networks.	5	
2305	Remote Access - VPN (Virtual Private Network)	The Supplier shall ensure the following controls are enforced for staff to connect to organisational networks and systems using Remote Access technologies, for example VPN: i) Enable MFA prior to establishing a remote connection to the network ii) Encrypt all data transmitted over a VPN connection iii) Disable split-tunnelling to ensure all Data is only transmitted via organisation controlled channels.	Functional	Intersects With	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	5	
2305	Remote Access - VPN (Virtual Private Network)	The Supplier shall ensure the following controls are enforced for staff to connect to organisational networks and systems using Remote Access technologies, for example VPN: i) Enable MFA prior to establishing a remote connection to the network ii) Encrypt all data transmitted over a VPN connection iii) Disable split-tunnelling to ensure all Data is only transmitted via organisation controlled channels.	Functional	Intersects With	Protection of Confidentiality / Integrity Using Encryption	NET-14.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	5	
2305	Remote Access - VPN (Virtual Private Network)	The Supplier shall ensure the following controls are enforced for staff to connect to organisational networks and systems using Remote Access technologies, for example VPN: i) Enable MFA prior to establishing a remote connection to the network ii) Encrypt all data transmitted over a VPN connection iii) Disable split-tunnelling to ensure all Data is only transmitted via organisation controlled channels.	Functional	Intersects With	Work From Anywhere (WFA) - Telecommuting Security	NET-14.5	Mechanisms exist to define secure telecommuting practices and govern remote access to Technology Assets, Applications, Services and/or Data (TAASD) for remote workers.	5	
2306	Remote Access Sessions	The Supplier shall employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Functional	Intersects With	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	8	
2306	Remote Access Sessions	The Supplier shall employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Functional	Subset Of	Protection of Confidentiality / Integrity Using Encryption	NET-14.2	Cryptographic mechanisms exist to protect the confidentiality and integrity of remote access sessions (e.g., VPN).	10	
2307	Managed Access Control Points	The Supplier shall route remote access via managed access control points.	Functional	Subset Of	Managed Access Control Points	NET-14.3	Mechanisms exist to route all remote accesses through managed network access control points (e.g., VPN concentrator).	10	
2308	Stored Data	The Supplier shall appropriately protect the confidentiality of soft and hard copies of data being stored for all Functions.	Functional	Subset Of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
2308	Stored Data	The Supplier shall appropriately protect the confidentiality of soft and hard copies of data being stored for all Functions.	Functional	Intersects With	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is processed and/or stored.	5	
2308	Stored Data	The Supplier shall appropriately protect the confidentiality of soft and hard copies of data being stored for all Functions.	Functional	Intersects With	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	5	
2309	Mobile Data	The Supplier shall protect, such as through encryption, data important to the operation of Functions and all Data on mobile devices.	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
2309	Mobile Data	The Supplier shall protect, such as through encryption, data important to the operation of Functions and all Data on mobile devices.	Functional	Intersects With	Full Device & Container-Based Encryption	MDM-03	Cryptographic mechanisms exist to protect the confidentiality and integrity of information on mobile devices through full-device or container encryption.	5	
2310	Removable Media	The Supplier shall: i) Maintain and manage an inventory of corporately owned removable storage media and devices ii) Encrypt removable media using secured and industry best practice methods iii) Allow only corporately owned and/or authorised removable storage media and devices to have read/write permissions iv) Prohibit the use of removable storage media and devices that are not corporately owned or authorised.	Functional	Subset Of	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.	10	
2310	Removable Media	The Supplier shall: i) Maintain and manage an inventory of corporately owned removable storage media and devices ii) Encrypt removable media using secured and industry best practice methods iii) Allow only corporately owned and/or authorised removable storage media and devices to have read/write permissions iv) Prohibit the use of removable storage media and devices that are not corporately owned or authorised.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	

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
2310	Removable Media	The Supplier shall: i) Maintain and manage an inventory of corporately owned removable storage media and devices ii) Encrypt removable media using secured and industry best practice methods iii) Allow only corporately owned and/or authorised removable storage media and devices to have read/write permissions iv) Prohibit the use of removable storage media and devices that are not corporately owned or authorised.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
2310	Removable Media	The Supplier shall: i) Maintain and manage an inventory of corporately owned removable storage media and devices ii) Encrypt removable media using secured and industry best practice methods iii) Allow only corporately owned and/or authorised removable storage media and devices to have read/write permissions iv) Prohibit the use of removable storage media and devices that are not corporately owned or authorised.	Functional	Intersects With	Media Use	DCH-10	Mechanisms exist to restrict the use of types of digital media on systems or system components.	5	
2310	Removable Media	The Supplier shall: i) Maintain and manage an inventory of corporately owned removable storage media and devices ii) Encrypt removable media using secured and industry best practice methods iii) Allow only corporately owned and/or authorised removable storage media and devices to have read/write permissions iv) Prohibit the use of removable storage media and devices that are not corporately owned or authorised.	Functional	Intersects With	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5	
2311	Authorised Working Locations	The Supplier shall maintain and update a list of authorised working locations which are not the organisation's premise and communicate these locations to all employees and contractors.	Functional	Intersects With	Identifying Authorized Work Locations	HRS-14	Mechanisms exist to identify and document authorized working locations, including: (1) Designated on-premises, organization-controlled work locations; and (2) Other off-premises locations not under organization-control (e.g., work from home).	8	
2311	Authorised Working Locations	The Supplier shall maintain and update a list of authorised working locations which are not the organisation's premise and communicate these locations to all employees and contractors.	Functional	Intersects With	Communicating Authorized Work Locations	HRS-14.1	Mechanisms exist to communicate authorized work locations to organizational personnel.	8	
2312	Security At Alternate Working Locations	The Supplier shall employ technical security controls and educate users to reduce the security risks to employees while working outside the organisation's premise. Technical security controls for consideration may include, but are not limited to: i) Always-on VPN to protect data in-transit ii) Screen privacy protector to prevent shoulder surfing iii) Disabling USB ports on devices iv) Full disk encryption User awareness topics may include, but are not limited to: i) Risks of using public Wi-Fi ii) Avoid taking confidential phone calls within earshot of unauthorised individuals iii) Shoulder surfing iv) Avoid leaving devices unattended	Functional	Intersects With	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	
2312	Security At Alternate Working Locations	The Supplier shall employ technical security controls and educate users to reduce the security risks to employees while working outside the organisation's premise. Technical security controls for consideration may include, but are not limited to: i) Always-on VPN to protect data in-transit ii) Screen privacy protector to prevent shoulder surfing iii) Disabling USB ports on devices iv) Full disk encryption User awareness topics may include, but are not limited to: i) Risks of using public Wi-Fi ii) Avoid taking confidential phone calls within earshot of unauthorised individuals iii) Shoulder surfing iv) Avoid leaving devices unattended	Functional	Intersects With	Alternate Work Site	PES-11	Physical security mechanisms exist to utilize appropriate management, operational and technical controls at alternate work sites.	5	
2313	Media/Equiment Sanitisation	The Supplier shall appropriately sanitise before reuse and / or disposal the devices, equipment, and removable storage media & devices holding data important to the operation of business Functions and that protect all Data.	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.	5	
2314	Ensure UK GDPR Compliance	The Supplier shall ensure that the processing of personal data is conducted in compliance with the General Data Protection Regulation.	Functional	Subset Of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
2315	Email Authentication Methods	The Supplier shall implement Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) to verify the authenticity of an email's source.	Functional	Intersects With	Domain Name Service (DNS) Resolution	NET-10	Mechanisms exist to ensure Domain Name Service (DNS) resolution is designed, implemented and managed to protect the security of name / address resolution.	5	
2315	Email Authentication Methods	The Supplier shall implement Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) to verify the authenticity of an email's source.	Functional	Intersects With	Sender Policy Framework (SPF)	NET-10.3	Mechanisms exist to validate the legitimacy of email communications through configuring a Domain Naming Service (DNS) Sender Policy Framework (SPF) record to specify the IP addresses and/or hostnames that are authorized to send email from the specified domain.	5	
2315	Email Authentication Methods	The Supplier shall implement Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) to verify the authenticity of an email's source.	Functional	Intersects With	Domain-Based Message Authentication Reporting and Conformance (DMARC)	NET-20.4	Mechanisms exist to implement domain signature verification protections that authenticate incoming email according to the Domain-based Message Authentication Reporting and Conformance (DMARC).	5	
2316	Personal and/or Personally Identifiable Information (PII) Processing/Transparency - Control Flow	The Supplier shall employ systems to monitor and control the flow of all Personal and/or Personally Identifiable Information (PII) and all government information (e.g. OFFICIAL and above) provided or produced during the contract throughout the information lifecycle in accordance with approved authorisations, required legislation and contractual requirements.	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	
2316	Personal and/or Personally Identifiable Information (PII) Processing/Transparency - Control Flow	The Supplier shall employ systems to monitor and control the flow of all Personal and/or Personally Identifiable Information (PII) and all government information (e.g. OFFICIAL and above) provided or produced during the contract throughout the information lifecycle in accordance with approved authorisations, required legislation and contractual requirements.	Functional	Intersects With	Personal Data (PD)	NET-03.4	Mechanisms exist to apply network-based processing rules to data elements of Personal Data (PD).	5	
2317	Endpoint Encryption	The Supplier shall implement and maintain full disk level encryption on all endpoints to industry standard solutions, for example, full disk encryption solutions using AES-256 encryption algorithm or FIPS equivalent.	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
2317	Endpoint Encryption	The Supplier shall implement and maintain full disk level encryption on all endpoints to industry standard solutions, for example, full disk encryption solutions using AES-256 encryption algorithm or FIPS equivalent.	Functional	Intersects With	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
2317	Endpoint Encryption	The Supplier shall implement and maintain full disk level encryption on all endpoints to industry standard solutions, for example, full disk encryption solutions using AES-256 encryption algorithm or FIPS equivalent.	Functional	Subset Of	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	10	
2318	Approved Cryptographic Methods	The Supplier shall employ appropriate nationally or departmentally approved cryptography when used to protect all Data (e.g. FIPS 140-2 or comparable standards)	Functional	Subset Of	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	10	
2319	Securely Manage Cryptographic Keys	The Supplier shall establish and manage cryptographic keys for cryptography employed in organisational systems using appropriate nationally or departmentally approved solutions (e.g. FIPS 140-2 or comparable standards)	Functional	Intersects With	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
2320	Data Loss Prevention (DLP)	The Supplier shall implement and maintain appropriate tooling to monitor and restrict the access and use of: i) Removable storage media and devices ii) External websites iii) Email	Functional	Intersects With	Data Loss Prevention (DLP)	NET-17	Automated mechanisms exist to implement Data Loss Prevention (DLP) to protect sensitive information as it is stored, transmitted and processed.	5	
2321	Publicly Accessible Data	The Supplier shall: i) Designate individuals authorised to make information publicly accessible ii) Train authorised individuals to ensure that publicly accessible information does not contain non-public information iii) Review the proposed content of information prior to posting onto the publicly accessible system to ensure that non-public information is not included iv) Periodically review the content on the publicly accessible system for non-public information and remove such information, if discovered.	Functional	Intersects With	Publicly Accessible Content	DCH-15	Mechanisms exist to control publicly-accessible content.	5	
2321	Publicly Accessible Data	The Supplier shall: i) Designate individuals authorised to make information publicly accessible ii) Train authorised individuals to ensure that publicly accessible information does not contain non-public information iii) Review the proposed content of information prior to posting onto the publicly accessible system to ensure that non-public information is not included iv) Periodically review the content on the publicly accessible system for non-public information and remove such information, if discovered.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
2321	Publicly Accessible Data	The Supplier shall: i) Designate individuals authorised to make information publicly accessible ii) Train authorised individuals to ensure that publicly accessible information does not contain non-public information iii) Review the proposed content of information prior to posting onto the publicly accessible system to ensure that non-public information is not included iv) Periodically review the content on the publicly accessible system for non-public information and remove such information, if discovered.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	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	
2321	Publicly Accessible Data	The Supplier shall: i) Designate individuals authorised to make information publicly accessible ii) Train authorised individuals to ensure that publicly accessible information does not contain non-public information iii) Review the proposed content of information prior to posting onto the publicly accessible system to ensure that non-public information is not included iv) Periodically review the content on the publicly accessible system for non-public information and remove such information, if discovered.	Functional	Intersects With	Publicly Accessible Content Reviews	WEB-14	Mechanisms exist to routinely review the content on publicly accessible systems for sensitive/regulated data and remove such information, if discovered.	5	
2322	Mobile Devices/Bring Your Own Device (BYOD)	The Supplier shall ensure that mobile devices accessing its corporate environment/data are appropriately configured and managed using industry recognised solutions such as Mobile Device Management (MDM) tooling.	Functional	Intersects With	Bring Your Own Device (BYOD) Usage	AST-16	Mechanisms exist to implement and govern a Bring Your Own Device (BYOD) program to reduce risk associated with personally-owned devices in the workplace.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2322	Mobile Devices/Bring Your Own Device (BYOD)	The Supplier shall ensure that mobile devices accessing its corporate environment/data are appropriately configured and managed using industry recognised solutions such as Mobile Device Management (MDM) tooling.	Functional	Intersects With	Use of Mobile Devices	HRS-05.5	Mechanisms exist to manage business risks associated with permitting mobile device access to organizational resources.	5	
2322	Mobile Devices/Bring Your Own Device (BYOD)	The Supplier shall ensure that mobile devices accessing its corporate environment/data are appropriately configured and managed using industry recognised solutions such as Mobile Device Management (MDM) tooling.	Functional	Subset Of	Centralized Management Of Mobile Devices	MDM-01	Mechanisms exist to implement and govern Mobile Device Management (MDM) controls.	10	
2323	Secure Destruction	The Supplier shall, where not otherwise stated explicitly by country, legislation or Authority instructions, implement procedures to ensure that all Data is securely destroyed when no longer needed, or at the expiration or termination of the Agreement. Supplier shall: i) Secure and confirm the erasure of Data from its systems and servers, including any physical or electronic copies, prior to asset destruction and disposal ii) Provide attestation of destruction, where specified by contract with Authority iii) Require that any third parties engaged to process the Data shall securely dispose of such Data when no longer needed to provide the service, unless otherwise stated explicitly by country, legislation or Authority instructions.	Functional	Subset Of	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	10	
2323	Secure Destruction	The Supplier shall, where not otherwise stated explicitly by country, legislation or Authority instructions, implement procedures to ensure that all Data is securely destroyed when no longer needed, or at the expiration or termination of the Agreement. Supplier shall: i) Secure and confirm the erasure of Data from its systems and servers, including any physical or electronic copies, prior to asset destruction and disposal ii) Provide attestation of destruction, where specified by contract with Authority iii) Require that any third parties engaged to process the Data shall securely dispose of such Data when no longer needed to provide the service, unless otherwise stated explicitly by country, legislation or Authority instructions.	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.	5	
2323	Secure Destruction	The Supplier shall, where not otherwise stated explicitly by country, legislation or Authority instructions, implement procedures to ensure that all Data is securely destroyed when no longer needed, or at the expiration or termination of the Agreement. Supplier shall: i) Secure and confirm the erasure of Data from its systems and servers, including any physical or electronic copies, prior to asset destruction and disposal ii) Provide attestation of destruction, where specified by contract with Authority iii) Require that any third parties engaged to process the Data shall securely dispose of such Data when no longer needed to provide the service, unless otherwise stated explicitly by country, legislation or Authority instructions.	Functional	Intersects With	System Media Sanitization Documentation	DCH-09.1	Mechanisms exist to supervise, track, document and verify system media sanitization and disposal actions.	5	
2323	Secure Destruction	The Supplier shall, where not otherwise stated explicitly by country, legislation or Authority instructions, implement procedures to ensure that all Data is securely destroyed when no longer needed, or at the expiration or termination of the Agreement. Supplier shall: i) Secure and confirm the erasure of Data from its systems and servers, including any physical or electronic copies, prior to asset destruction and disposal ii) Provide attestation of destruction, where specified by contract with Authority iii) Require that any third parties engaged to process the Data shall securely dispose of such Data when no longer needed to provide the service, unless otherwise stated explicitly by country, legislation or Authority instructions.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	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).	5	
2400	System Security	The Supplier shall ensure that network and information systems and technology critical for the operation of business Functions and protection of Data are protected from cyber attack. An organisational understanding of risk to business Functions and protection of Data informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
2400	System Security	The Supplier shall ensure that network and information systems and technology critical for the operation of business Functions and protection of Data are protected from cyber attack. An organisational understanding of risk to business Functions and protection of Data informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.	Functional	Subset Of	Secure Engineering Principles	SEA-01	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).	10	
2401	Secure Configuration	The Supplier shall securely configure the network and information systems that support the operation of business Functions and that protect Data.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
2402	Vulnerability Management	The Supplier shall implement a vulnerability and patch management process to identify, report, and remediate application and system (internal and external facing) vulnerabilities that is approved by the application or system owner and is commensurate with the level of risk by: i) Performing vulnerability scans on a monthly basis and during any major system or application updates ii) Implementing vendor patches or fixes prioritising using the CVSS v3 scoring iii) Developing a Risk Treatment Plan to address identified vulnerabilities. The Supplier shall address vulnerabilities in accordance with the Supplier's internal vulnerability remediation timelines and in line with reasonable industry standards for vulnerability management based on CVSS v3 or above.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
2402	Vulnerability Management	The Supplier shall implement a vulnerability and patch management process to identify, report, and remediate application and system (internal and external facing) vulnerabilities that is approved by the application or system owner and is commensurate with the level of risk by: i) Performing vulnerability scans on a monthly basis and during any major system or application updates ii) Implementing vendor patches or fixes prioritising using the CVSS v3 scoring iii) Developing a Risk Treatment Plan to address identified vulnerabilities. The Supplier shall address vulnerabilities in accordance with the Supplier's internal vulnerability remediation timelines and in line with reasonable industry standards for vulnerability management based on CVSS v3 or above.	Functional	Intersects With	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
2402	Vulnerability Management	The Supplier shall implement a vulnerability and patch management process to identify, report, and remediate application and system (internal and external facing) vulnerabilities that is approved by the application or system owner and is commensurate with the level of risk by: i) Performing vulnerability scans on a monthly basis and during any major system or application updates ii) Implementing vendor patches or fixes prioritising using the CVSS v3 scoring iii) Developing a Risk Treatment Plan to address identified vulnerabilities. The Supplier shall address vulnerabilities in accordance with the Supplier's internal vulnerability remediation timelines and in line with reasonable industry standards for vulnerability management based on CVSS v3 or above.	Functional	Intersects With	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
2402	Vulnerability Management	The Supplier shall implement a vulnerability and patch management process to identify, report, and remediate application and system (internal and external facing) vulnerabilities that is approved by the application or system owner and is commensurate with the level of risk by: i) Performing vulnerability scans on a monthly basis and during any major system or application updates ii) Implementing vendor patches or fixes prioritising using the CVSS v3 scoring iii) Developing a Risk Treatment Plan to address identified vulnerabilities. The Supplier shall address vulnerabilities in accordance with the Supplier's internal vulnerability remediation timelines and in line with reasonable industry standards for vulnerability management based on CVSS v3 or above.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
2403	Penetration Testing	The Supplier shall conduct penetration testing (minimum every 12 months) against externally facing systems used to support the operation of Functions and that protect Data. The penetration testing programme shall be based upon industry standards and performed by subject matter experts. The Supplier shall ensure that any deficiencies identified are remediated in a timely manner in line with their risk to the network. The Supplier shall retain records including: i) The scope and methodology utilised ii) The number of critical, high, and medium severity findings iii) The name of the tester iv) The date of the testing v) Timelines and actions for a remedial plan.	Functional	Intersects With	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on Technology Assets, Applications and/or Services (TAAS).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2404	Change Management	The Supplier shall formally document, publish and review (minimum every 12 months) the change control procedures to manage changes to information systems, supporting infrastructure and facilities. The change management policy includes: i) Definitions of the types of change (e.g. standard, critical, emergency) with associated processes ii) Roles and responsibilities for those involved in the change or approving the change. Prior to implementing any changes, Supplier shall: i) Establish acceptance criteria for production change approval and implementation ii) Require stakeholder approval prior to any change implementation iii) Formally record the change in a centralised repository iv) Document business impact analysis outcomes and document back-out procedures should the change fail v) Keep a full audit trail of the change request, testing conducted, associated documentation, approvals and outcomes vi) Document and record security impact analysis outcomes along with any mitigating actions.	Functional	Subset Of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
2405	Patch Management	The Supplier shall develop and maintain an appropriately robust patch management programme to address known vulnerabilities on its network within industry best-practice timelines. The Supplier shall take appropriate steps to identify, assess, test and implement patches for endpoints, network devices and software which address known vulnerabilities within industry best practice timeline. The Supplier shall have appropriate processes in place to address out-of-band emergency patching and/or mitigating actions.	Functional	Subset Of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
2405	Patch Management	The Supplier shall develop and maintain an appropriately robust patch management programme to address known vulnerabilities on its network within industry best-practice timelines. The Supplier shall take appropriate steps to identify, assess, test and implement patches for endpoints, network devices and software which address known vulnerabilities within industry best practice timeline. The Supplier shall have appropriate processes in place to address out-of-band emergency patching and/or mitigating actions.	Functional	Subset Of	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	10	
2405	Patch Management	The Supplier shall develop and maintain an appropriately robust patch management programme to address known vulnerabilities on its network within industry best-practice timelines. The Supplier shall take appropriate steps to identify, assess, test and implement patches for endpoints, network devices and software which address known vulnerabilities within industry best practice timeline. The Supplier shall have appropriate processes in place to address out-of-band emergency patching and/or mitigating actions.	Functional	Intersects With	Pre-Deployment Patch Testing	VPM-05.6	Mechanisms exist to perform due diligence on software and/or firmware update stability by conducting pre-production testing in a non-production environment.	5	
2405	Patch Management	The Supplier shall develop and maintain an appropriately robust patch management programme to address known vulnerabilities on its network within industry best-practice timelines. The Supplier shall take appropriate steps to identify, assess, test and implement patches for endpoints, network devices and software which address known vulnerabilities within industry best practice timeline. The Supplier shall have appropriate processes in place to address out-of-band emergency patching and/or mitigating actions.	Functional	Intersects With	Out-of-Cycle Patching	VPM-05.7	Mechanisms exist to perform out-of-cycle software and/or firmware updates to address time-sensitive remediations.	5	
2406	Privacy Warning Notices - Prior To Access	The Supplier shall ensure that mechanisms are in place to ensure users accept appropriate warning notices prior to information system access. At a minimum users must be warned that: i) Use of the information system is monitored, recorded and subject to audit ii) Unauthorised usage of the information system is prohibited iii) Unauthorised usage of the information system use is subject to criminal and civil penalties iv) In continuing, the user affirms consent to monitoring and recording of their activities	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
2406	Privacy Warning Notices - Prior To Access	The Supplier shall ensure that mechanisms are in place to ensure users accept appropriate warning notices prior to information system access. At a minimum users must be warned that: i) Use of the information system is monitored, recorded and subject to audit ii) Unauthorised usage of the information system is prohibited iii) Unauthorised usage of the information system use is subject to criminal and civil penalties iv) In continuing, the user affirms consent to monitoring and recording of their activities	Functional	Intersects With	System Use Notification (Logon Banner)	SEA-18	Mechanisms exist to utilize system use notification / logon banners that display an approved system use notification message or banner before granting access to Technology Assets, Applications and/or Services (TAAS).	5	
2407	Privacy Warning Notices - Specific Handling	The Supplier shall ensure that users accept appropriate warning notices prior to information system access where information systems contain information with specific handling requirements imposed by the UK or its International Partners. Such warnings must only be provided to authenticated users. At a minimum users must be warned that: i) The information system contains information with specific requirements imposed by the UK and/or international partner nations. ii) Use of the information system may be subject to other specified requirements associated with certain types of information, such as that subject to Export Controls or licences.	Functional	Intersects With	Data Privacy Notice	PRI-02	Mechanisms exist to: (1) Make data privacy notice(s) available to individuals upon first interacting with an organization and subsequently as necessary; (2) Ensure that data privacy notices are clear and easy-to-understand, expressing relevant information about how Personal Data (PD) is collected, received, processed, stored, transmitted, shared, updated and/or disposed; (3) Contain all necessary notice-related criteria required by applicable statutory, regulatory and contractual obligations; (4) Define the scope of PD processing activities, including the geographic locations and third-party recipients that process the PD within the scope of the data privacy notice; (5) Periodically, review and update the content of the privacy notice, as necessary; and (6) Retain prior versions of the privacy notice, in accordance with data retention requirements.	5	
2407	Privacy Warning Notices - Specific Handling	The Supplier shall ensure that users accept appropriate warning notices prior to information system access where information systems contain information with specific handling requirements imposed by the UK or its International Partners. Such warnings must only be provided to authenticated users. At a minimum users must be warned that: i) The information system contains information with specific requirements imposed by the UK and/or international partner nations. ii) Use of the information system may be subject to other specified requirements associated with certain types of information, such as that subject to Export Controls or licences.	Functional	Intersects With	System Use Notification (Logon Banner)	SEA-18	Mechanisms exist to utilize system use notification / logon banners that display an approved system use notification message or banner before granting access to Technology Assets, Applications and/or Services (TAAS).	5	
2408	Screen Locking/Timeouts	The Supplier shall have controls in place to automatically lock user sessions after a predefined period. The lock screen shall conceal all information previously displayed on the screen and prevent unauthorised viewing of data.	Functional	Intersects With	Session Lock	IAC-24	Mechanisms exist to initiate a session lock after an organization-defined time period of inactivity, or upon receiving a request from a user and retain the session lock until the user reestablishes access using established identification and authentication methods.	5	
2409	Identify Allowed Programs	The Supplier shall identify software programs authorised to execute on the corporate environment. For all other programs employ a block by default, permit-by-exception policy.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
2410	Review the List of Approved Software	The Supplier shall review and manage the list of authorised software programs at least every 90 days.	Functional	Intersects With	Approved Technologies	AST-01.4	Mechanisms exist to maintain a current list of approved technologies (hardware and software).	5	
2411	Secured Internet Access	The Supplier shall ensure the following internet controls are enforced on endpoints: i) Technical controls to prevent malware infection from internet browsing are in place ii) Block undesirable websites from being accessed (e.g. malicious sites, inappropriate content etc.) iii) Prevent code being launched on the corporate host iv) Prevent downloads to the corporate host from the internet without sandboxing and anti-malware scan v) Automatically block suspicious traffic and communications vi) Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. Ensure auditing is enabled for these controls and security operators are notified of the attempted above actions. Where users have a necessity to perform the above activities, ensure a robust model and supporting processes and technologies are employed to mitigate the additional risk (e.g. allow/block listing, network monitoring, vulnerability scanning etc.)	Functional	Subset Of	Endpoint Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Endpoint Device Management (EDM) controls.	10	
2411	Secured Internet Access	The Supplier shall ensure the following internet controls are enforced on endpoints: i) Technical controls to prevent malware infection from internet browsing are in place ii) Block undesirable websites from being accessed (e.g. malicious sites, inappropriate content etc.) iii) Prevent code being launched on the corporate host iv) Prevent downloads to the corporate host from the internet without sandboxing and anti-malware scan v) Automatically block suspicious traffic and communications vi) Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. Ensure auditing is enabled for these controls and security operators are notified of the attempted above actions. Where users have a necessity to perform the above activities, ensure a robust model and supporting processes and technologies are employed to mitigate the additional risk (e.g. allow/block listing, network monitoring, vulnerability scanning etc.)	Functional	Intersects With	Endpoint Protection Measures	END-02	Mechanisms exist to protect the confidentiality, integrity, availability and safety of endpoint devices.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2411	Secured Internet Access	The Supplier shall ensure the following internet controls are enforced on endpoints: i) Technical controls to prevent malware infection from internet browsing are in place ii) Block undesirable websites from being accessed (e.g. malicious sites, inappropriate content etc.) iii) Prevent code being launched on the corporate host iv) Prevent downloads to the corporate host from the internet without sandboxing and anti-malware scan v) Automatically block suspicious traffic and communications vi) Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. Ensure auditing is enabled for these controls and security operators are notified of the attempted above actions. Where users have a necessity to perform the above activities, ensure a robust model and supporting processes and technologies are employed to mitigate the additional risk (e.g. allow/block listing, network monitoring, vulnerability scanning etc.)	Functional	Intersects With	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
2411	Secured Internet Access	The Supplier shall ensure the following internet controls are enforced on endpoints: i) Technical controls to prevent malware infection from internet browsing are in place ii) Block undesirable websites from being accessed (e.g. malicious sites, inappropriate content etc.) iii) Prevent code being launched on the corporate host iv) Prevent downloads to the corporate host from the internet without sandboxing and anti-malware scan v) Automatically block suspicious traffic and communications vi) Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. Ensure auditing is enabled for these controls and security operators are notified of the attempted above actions. Where users have a necessity to perform the above activities, ensure a robust model and supporting processes and technologies are employed to mitigate the additional risk (e.g. allow/block listing, network monitoring, vulnerability scanning etc.)	Functional	Intersects With	Detonation Chambers (Sandboxes)	IRO-15	Mechanisms exist to utilize a detonation chamber capability to detect and/or block potentially-malicious files and email attachments.	5	
2411	Secured Internet Access	The Supplier shall ensure the following internet controls are enforced on endpoints: i) Technical controls to prevent malware infection from internet browsing are in place ii) Block undesirable websites from being accessed (e.g. malicious sites, inappropriate content etc.) iii) Prevent code being launched on the corporate host iv) Prevent downloads to the corporate host from the internet without sandboxing and anti-malware scan v) Automatically block suspicious traffic and communications vi) Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. Ensure auditing is enabled for these controls and security operators are notified of the attempted above actions. Where users have a necessity to perform the above activities, ensure a robust model and supporting processes and technologies are employed to mitigate the additional risk (e.g. allow/block listing, network monitoring, vulnerability scanning etc.)	Functional	Intersects With	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	
2411	Secured Internet Access	The Supplier shall ensure the following internet controls are enforced on endpoints: i) Technical controls to prevent malware infection from internet browsing are in place ii) Block undesirable websites from being accessed (e.g. malicious sites, inappropriate content etc.) iii) Prevent code being launched on the corporate host iv) Prevent downloads to the corporate host from the internet without sandboxing and anti-malware scan v) Automatically block suspicious traffic and communications vi) Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. Ensure auditing is enabled for these controls and security operators are notified of the attempted above actions. Where users have a necessity to perform the above activities, ensure a robust model and supporting processes and technologies are employed to mitigate the additional risk (e.g. allow/block listing, network monitoring, vulnerability scanning etc.)	Functional	Intersects With	Network Connection Termination	NET-07	Mechanisms exist to terminate network connections at the end of a session or after an organization-defined time period of inactivity.	5	
2411	Secured Internet Access	The Supplier shall ensure the following internet controls are enforced on endpoints: i) Technical controls to prevent malware infection from internet browsing are in place ii) Block undesirable websites from being accessed (e.g. malicious sites, inappropriate content etc.) iii) Prevent code being launched on the corporate host iv) Prevent downloads to the corporate host from the internet without sandboxing and anti-malware scan v) Automatically block suspicious traffic and communications vi) Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. Ensure auditing is enabled for these controls and security operators are notified of the attempted above actions. Where users have a necessity to perform the above activities, ensure a robust model and supporting processes and technologies are employed to mitigate the additional risk (e.g. allow/block listing, network monitoring, vulnerability scanning etc.)	Functional	Intersects With	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
2412	Voice over Internet Protocol (VoIP)	The Supplier should establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and ensure controls are in place to authorise, monitor, and control the use of VoIP within the information system.	Functional	Subset Of	Voice Over Internet Protocol (VoIP) Security	AST-21	Mechanisms exist to implement secure Internet Protocol Telephony (IPT) that logically or physically separates Voice Over Internet Protocol (VoIP) traffic from data networks.	10	
2413	Mobile Code Management	The Supplier shall define acceptable and unacceptable mobile code, and ensure controls are in place to identify, authorise, monitor, review and control the use of mobile code within the organisation.	Functional	Subset Of	Mobile Code	END-10	Mechanisms exist to address mobile code / operating system-independent applications.	10	
2414	Communication Authenticity Protection	The Supplier shall use secure network management and communication protocols to protect session authenticity addressing communications protection at the session level.	Functional	Intersects With	Session Integrity	NET-09	Mechanisms exist to protect the authenticity and integrity of communications sessions.	5	
2415	Automatically Identify and Address Misconfigurations and Unauthorised Components	The Supplier shall employ automated mechanisms to detect misconfigured or unauthorised system components.	Functional	Subset Of	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of Technology Assets, Applications and/or Services (TAAS) through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	10	
2416	Shared System Resources	The supplier shall prevent unauthorised and unintended information transfer via shared system resources (e.g. registers, cache memory, main memory, hard disks).	Functional	Intersects With	Information In Shared Resources	SEA-05	Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.	5	
2417	Authorise Remote Execution of Privileged Commands	The Supplier shall ensure that all remote users acquire appropriate authorisation prior to accessing and/or executing privileged functions.	Functional	Intersects With	Remote Privileged Commands & Sensitive Data Access	NET-14.4	Mechanisms exist to restrict the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs.	5	
2418	Baseline Configurations and Inventories	The Supplier shall implement, update and document system hardening procedures. Implement, update and document baseline configurations settings for all information technology products deployed in organisational systems; this shall include the restriction of user actions and of unsupported software and hardware.	Functional	Intersects With	Secure 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	
2418	Baseline Configurations and Inventories	The Supplier shall implement, update and document system hardening procedures. Implement, update and document baseline configurations settings for all information technology products deployed in organisational systems; this shall include the restriction of user actions and of unsupported software and hardware.	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	8	
2418	Baseline Configurations and Inventories	The Supplier shall implement, update and document system hardening procedures. Implement, update and document baseline configurations settings for all information technology products deployed in organisational systems; this shall include the restriction of user actions and of unsupported software and hardware.	Functional	Intersects With	Baseline Tailoring	CFG-02.9	Mechanisms exist to allow baseline controls to be specialized or customized by applying a defined set of tailoring actions that are specific to: (1) Mission / business functions; (2) Operational environment; (3) Specific threats or vulnerabilities; or (4) Other conditions or situations that could affect mission / business success.	5	
2419	Obscure Authentication Information	The Supplier shall configure systems to obscure authentication information, for example, passwords to ensure that they are not displayed as cleartext when a user is inputting their credentials.	Functional	Intersects With	Authenticator Feedback	IAC-11	Mechanisms exist to obscure the feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	8	
2420	Authentication Feedback	The Supplier shall configure systems to minimise feedback information from failed logons to ensure that the system does not provide any information that would allow unauthorised individuals to compromise authentication mechanisms. e.g. explicitly stating that the password is the incorrect authentication component.	Functional	Intersects With	Authenticator Feedback	IAC-11	Mechanisms exist to obscure the feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	5	
2421	Network Time Protocol (NTP)	The Supplier shall implement a Network Time Protocol (NTP) to a recognised authoritative source, to synchronise the clocks of every network device to ensure accurate and consistent timestamps for audit records on associated system logs.	Functional	Intersects With	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	8	
2421	Network Time Protocol (NTP)	The Supplier shall implement a Network Time Protocol (NTP) to a recognised authoritative source, to synchronise the clocks of every network device to ensure accurate and consistent timestamps for audit records on associated system logs.	Functional	Intersects With	Clock Synchronization	SEA-20	Mechanisms exist to utilize time-synchronization technology to synchronize all critical system clocks.	8	
2422	Physical and Logical Access Restrictions	The Supplier shall define, document, approve, and enforce physical and logical access restrictions associated with changes to organisational systems.	Functional	Intersects With	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
2422	Physical and Logical Access Restrictions	The Supplier shall define, document, approve, and enforce physical and logical access restrictions associated with changes to organisational systems.	Functional	Subset Of	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	10	
2422	Physical and Logical Access Restrictions	The Supplier shall define, document, approve, and enforce physical and logical access restrictions associated with changes to organisational systems.	Functional	Subset Of	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	10	
2423	Trusted Source Repository	The Supplier shall identify, register and maintain an inventory of system components using automated tooling for those assets that support business Functions and protect Data in an asset register, and at a minimum, include data location and asset ownership information.	Functional	Intersects With	Configuration Management Database (CMDB)	AST-02.9	Mechanisms exist to implement and manage a Configuration Management Database (CMDB), or similar technology, to monitor and govern technology asset-specific information.	8	

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
2424	Implement Audit for Stored Credentials Outside Policy	The Supplier shall ensure administrator credentials are stored through an approved and secured storage mechanism (process/location/tools etc.) and quarterly audits are performed to ensure the control is consistently applied and functions appropriately.	Functional	Intersects With	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	5	
2424	Implement Audit for Stored Credentials Outside Policy	The Supplier shall ensure administrator credentials are stored through an approved and secured storage mechanism (process/location/tools etc.) and quarterly audits are performed to ensure the control is consistently applied and functions appropriately.	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	
2424	Implement Audit for Stored Credentials Outside Policy	The Supplier shall ensure administrator credentials are stored through an approved and secured storage mechanism (process/location/tools etc.) and quarterly audits are performed to ensure the control is consistently applied and functions appropriately.	Functional	Intersects With	Privileged Account Inventories	IAC-16.1	Mechanisms exist to inventory all privileged accounts and validate that each person with elevated privileges is authorized by the appropriate level of organizational management.	5	
2425	Use Integrity Verification Tools	The Supplier shall implement an integrity verification tool to detect unauthorised changes to web-facing, critical software and firmware. Upon discovering discrepancies, the tool should automatically trigger the incident response process.	Functional	Intersects With	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	5	
2425	Use Integrity Verification Tools	The Supplier shall implement an integrity verification tool to detect unauthorised changes to web-facing, critical software and firmware. Upon discovering discrepancies, the tool should automatically trigger the incident response process.	Functional	Intersects With	Integrity Checks	END-06.1	Mechanisms exist to validate configurations through integrity checking of software and firmware.	5	
2426	Anti-Malware Capabilities	The Supplier shall ensure that anti-malware capabilities are regularly audited, to verify they are up to date, functional (e.g. performing real-time scans as well as periodic scans), managed, detect malware, report detections and update both malware signatures and software when new releases are available.	Functional	Subset Of	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	
2426	Anti-Malware Capabilities	The Supplier shall ensure that anti-malware capabilities are regularly audited, to verify they are up to date, functional (e.g. performing real-time scans as well as periodic scans), managed, detect malware, report detections and update both malware signatures and software when new releases are available.	Functional	Intersects With	Automatic Antimalware Signature Updates	END-04.1	Automated mechanisms exist to update antimalware technologies, including signature definitions.	5	
2426	Anti-Malware Capabilities	The Supplier shall ensure that anti-malware capabilities are regularly audited, to verify they are up to date, functional (e.g. performing real-time scans as well as periodic scans), managed, detect malware, report detections and update both malware signatures and software when new releases are available.	Functional	Intersects With	Always On Protection	END-04.7	Mechanisms exist to ensure that anti-malware technologies are continuously running in real-time and cannot be disabled or altered by non-privileged users, unless specifically authorized by management on a case-by-case basis for a limited time period.	8	
2427	Monitor/Protect Communications at Boundaries	The Supplier shall monitor, control, and protect communications (information transmitted or received by organisational systems) at the external boundaries except as prohibited by Applicable Law and key internal boundaries of those organisational systems. This includes all staff including all remote workers to carry out their duties.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
2427	Monitor/Protect Communications at Boundaries	The Supplier shall monitor, control, and protect communications (information transmitted or received by organisational systems) at the external boundaries except as prohibited by Applicable Law and key internal boundaries of those organisational systems. This includes all staff including all remote workers to carry out their duties.	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	
2428	Verify/Limit Access to External System Connections	The Supplier shall control and limit connections to external systems by an allow-list on the network boundary.	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	
2430	External System Connection Review	The Supplier shall promptly remove or disable unnecessary firewall rules when they are no longer required or fulfil no business need.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	8	
2430	External System Connection Review	The Supplier shall promptly remove or disable unnecessary firewall rules when they are no longer required or fulfil no business need.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	8	
2500	Resilient Networks and Systems	The Supplier shall build resilience against cyber-attack and system failure into their design, implementation, operation and management of systems that support the operation of business Functions and protection of Data.	Functional	Intersects With	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	8	
2501	Design for Resilience	The Supplier shall design the network and information systems supporting their Functions and protect Data to be resilient to cyber security incidents and system failure. Systems shall be appropriately segregated and resource limitations mitigated.	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	
2501	Design for Resilience	The Supplier shall design the network and information systems supporting their Functions and protect Data to be resilient to cyber security incidents and system failure. Systems shall be appropriately segregated and resource limitations mitigated.	Functional	Intersects With	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	8	
2503	Resilience Preparation With Testing	The Supplier shall develop recovery plans for all systems that deliver Functions and protect Data. Recovery plans must also be tested at least annually with any deficiencies being recorded, risk assessed and resolved within defined timelines.	Functional	Intersects With	Contingency Plan Testing & Exercises	BCD-04	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	
2505	Resilient Backups	The Supplier shall hold accessible and secured current backups of data and information needed to recover operation of their Functions and protect Data. Backup procedures and media shall include: i) Appropriate encryption technology ii) Integrity validation iii) Secure offsite storage supporting availability requirements iv) Regular backup recovery testing.	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	
2505	Resilient Backups	The Supplier shall hold accessible and secured current backups of data and information needed to recover operation of their Functions and protect Data. Backup procedures and media shall include: i) Appropriate encryption technology ii) Integrity validation iii) Secure offsite storage supporting availability requirements iv) Regular backup recovery testing.	Functional	Intersects With	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	8	
2505	Resilient Backups	The Supplier shall hold accessible and secured current backups of data and information needed to recover operation of their Functions and protect Data. Backup procedures and media shall include: i) Appropriate encryption technology ii) Integrity validation iii) Secure offsite storage supporting availability requirements iv) Regular backup recovery testing.	Functional	Intersects With	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	5	
2505	Resilient Backups	The Supplier shall hold accessible and secured current backups of data and information needed to recover operation of their Functions and protect Data. Backup procedures and media shall include: i) Appropriate encryption technology ii) Integrity validation iii) Secure offsite storage supporting availability requirements iv) Regular backup recovery testing.	Functional	Intersects With	Test Restoration Using Sampling	BCD-11.5	Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.	5	
2506	Physical Transport of Backups	The Supplier shall protect the physical movement of media containing Data in transit using the following methodologies: i) Store backup media within a secured and locked container prior to transport. ii) Utilise a certified backup courier to transport backup drives/tapes. iii) Maintain a full chain of custody record. iv) Ensure that tracking information is recorded for all drives being transported. v) Implement appropriate cryptographic mechanisms to protect confidentiality.	Functional	Intersects With	Transfer to Alternate Storage Site	BCD-11.6	Mechanisms exist to transfer backup data to the alternate storage site at a rate that is capable of meeting both Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
2506	Physical Transport of Backups	The Supplier shall protect the physical movement of media containing Data in transit using the following methodologies: i) Store backup media within a secured and locked container prior to transport. ii) Utilise a certified backup courier to transport backup drives/tapes. iii) Maintain a full chain of custody record. iv) Ensure that tracking information is recorded for all drives being transported. v) Implement appropriate cryptographic mechanisms to protect confidentiality.	Functional	Intersects With	Cryptographic Protection	BCD-11.4	Cryptographic mechanisms exist to prevent the unauthorized disclosure and/or modification of backup information.	5	
2506	Physical Transport of Backups	The Supplier shall protect the physical movement of media containing Data in transit using the following methodologies: i) Store backup media within a secured and locked container prior to transport. ii) Utilise a certified backup courier to transport backup drives/tapes. iii) Maintain a full chain of custody record. iv) Ensure that tracking information is recorded for all drives being transported. v) Implement appropriate cryptographic mechanisms to protect confidentiality.	Functional	Intersects With	Media Transportation	DCH-07	Mechanisms exist to protect and control digital and non-digital media during transport outside of controlled areas using appropriate security measures.	5	
2507	Deny Traffic By Default at Interfaces	The Supplier shall ensure that firewalls must block every network connectivity path and network service not explicitly authorised by the appropriate Change Advisory Board (CAB). Traffic flow policy exceptions that are no longer supported by an explicit business need must be removed.	Functional	Intersects With	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	8	
2507	Deny Traffic By Default at Interfaces	The Supplier shall ensure that firewalls must block every network connectivity path and network service not explicitly authorised by the appropriate Change Advisory Board (CAB). Traffic flow policy exceptions that are no longer supported by an explicit business need must be removed.	Functional	Intersects With	Periodic Review	CFG-03.1	Mechanisms exist to periodically review system configurations to identify and disable unnecessary and/or non-secure functions, ports, protocols and services.	5	
2507	Deny Traffic By Default at Interfaces	The Supplier shall ensure that firewalls must block every network connectivity path and network service not explicitly authorised by the appropriate Change Advisory Board (CAB). Traffic flow policy exceptions that are no longer supported by an explicit business need must be removed.	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, permit by exception).	5	
2508	Separate Public and Internal Subnetworks	The Supplier shall implement network segmentation for publicly accessible system components to ensure logical and/or physical separation from internal network components.	Functional	Intersects With	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate Technology Assets, Applications and/or Services (TAAS) to protect from other network resources.	5	
2509	Managed Email Filtering	The Supplier shall implement appropriate tooling or methods to detect, block and report malicious or spam emails coming into the network. Such tooling or methods may include learning capabilities for more effectively identifying legitimate communications.	Functional	Subset Of	Phishing & Spam Protection	END-08	Mechanisms exist to utilize anti-phishing and spam protection technologies to detect and take action on unsolicited messages transported by electronic mail.	10	
2509	Managed Email Filtering	The Supplier shall implement appropriate tooling or methods to detect, block and report malicious or spam emails coming into the network. Such tooling or methods may include learning capabilities for more effectively identifying legitimate communications.	Functional	Intersects With	Adaptive Email Protections	NET-20.7	Mechanisms exist to utilize adaptive email protections that involve employing risk-based analysis in the application and enforcement of email protections.	5	
2510	Diagnostic Programmes	The Supplier shall check all media containing diagnostic and/or test programs for malicious code prior to use on the organisational network.	Functional	Intersects With	Inspect Media	MNT-04.2	Mechanisms exist to check media containing diagnostic and test programs for malicious code before the media are used.	5	
2511	Maintenance Activities	The Supplier shall ensure that relevant good practice tooling, techniques and mechanisms are authorised or provided to maintenance personnel in order to carry out their duties	Functional	Intersects With	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the Technology Asset, Application and/or Service (TAAS).	5	
2511	Maintenance Activities	The Supplier shall ensure that relevant good practice tooling, techniques and mechanisms are authorised or provided to maintenance personnel in order to carry out their duties	Functional	Intersects With	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes
2512	MFA for Remote Maintenance Activities	The Supplier shall require multi-factor authentication to establish non local maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	Functional	Subset Of	Multi-Factor Authentication (MFA)	IAC-06	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/regulated data.	10	
2512	MFA for Remote Maintenance Activities	The Supplier shall require multi-factor authentication to establish non local maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	Functional	Intersects With	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	5	
2513	Maintenance Personnel Supervision	The Supplier shall designate authorised, suitably qualified and experienced personnel to supervise maintenance personnel who do not possess the required physical access authorisations.	Functional	Intersects With	Maintenance Personnel Without Appropriate Access	MNT-06.1	Mechanisms exist to ensure the risks associated with maintenance personnel who do not have appropriate access authorizations, clearances or formal access approvals are appropriately mitigated.	5	
2600	Staff Awareness and Training	The Supplier shall ensure that 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 business Functions and protection of Data.	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	
2600	Staff Awareness and Training	The Supplier shall ensure that 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 business Functions and protection of Data.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	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	
2601	Cyber Security Culture	The Supplier shall develop and maintain a positive cyber security culture which encourages employees to make information security part of their day-to-day activities and incentivises them for doing so.	Functional	Intersects With	Risk Culture	RSK-12	Mechanisms exist to ensure teams are committed to a culture that considers and communicates technology-related risk.	5	
2601	Cyber Security Culture	The Supplier shall develop and maintain a positive cyber security culture which encourages employees to make information security part of their day-to-day activities and incentivises them for doing so.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	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	
2602	Cyber Security Training	The Supplier shall ensure that people who support the operation of Functions and protection of Data are appropriately trained in cyber security. The Supplier shall conduct awareness training at least every 12 months to recognise and respond to the following topics: i) Social engineering and phishing ii) Advanced persistent threats iii) Suspected breaches iv) Suspicious behaviours. A range of approaches to cyber security training, awareness and communications shall be employed and the Supplier shall update the training every 12 months or when there are significant changes to the threat.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	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	
2602	Cyber Security Training	The Supplier shall ensure that people who support the operation of Functions and protection of Data are appropriately trained in cyber security. The Supplier shall conduct awareness training at least every 12 months to recognise and respond to the following topics: i) Social engineering and phishing ii) Advanced persistent threats iii) Suspected breaches iv) Suspicious behaviours. A range of approaches to cyber security training, awareness and communications shall be employed and the Supplier shall update the training every 12 months or when there are significant changes to the threat.	Functional	Intersects With	Social Engineering & Mining	SAT-02.2	Mechanisms exist to include awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.	5	
2602	Cyber Security Training	The Supplier shall ensure that people who support the operation of Functions and protection of Data are appropriately trained in cyber security. The Supplier shall conduct awareness training at least every 12 months to recognise and respond to the following topics: i) Social engineering and phishing ii) Advanced persistent threats iii) Suspected breaches iv) Suspicious behaviours. A range of approaches to cyber security training, awareness and communications shall be employed and the Supplier shall update the training every 12 months or when there are significant changes to the threat.	Functional	Intersects With	Role-Based Security, Compliance & Resilience Training	SAT-03	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	
2602	Cyber Security Training	The Supplier shall ensure that people who support the operation of Functions and protection of Data are appropriately trained in cyber security. The Supplier shall conduct awareness training at least every 12 months to recognise and respond to the following topics: i) Social engineering and phishing ii) Advanced persistent threats iii) Suspected breaches iv) Suspicious behaviours. A range of approaches to cyber security training, awareness and communications shall be employed and the Supplier shall update the training every 12 months or when there are significant changes to the threat.	Functional	Intersects With	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	
2602	Cyber Security Training	The Supplier shall ensure that people who support the operation of Functions and protection of Data are appropriately trained in cyber security. The Supplier shall conduct awareness training at least every 12 months to recognise and respond to the following topics: i) Social engineering and phishing ii) Advanced persistent threats iii) Suspected breaches iv) Suspicious behaviours. A range of approaches to cyber security training, awareness and communications shall be employed and the Supplier shall update the training every 12 months or when there are significant changes to the threat.	Functional	Intersects With	Sensitive / Regulated Data Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive/regulated data is formally trained in data handling requirements.	5	
2602	Cyber Security Training	The Supplier shall ensure that people who support the operation of Functions and protection of Data are appropriately trained in cyber security. The Supplier shall conduct awareness training at least every 12 months to recognise and respond to the following topics: i) Social engineering and phishing ii) Advanced persistent threats iii) Suspected breaches iv) Suspicious behaviours. A range of approaches to cyber security training, awareness and communications shall be employed and the Supplier shall update the training every 12 months or when there are significant changes to the threat.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	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	
2603	Staff Risk Awareness	The Supplier shall ensure that managers, systems administrators, and users of organisational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organisational information systems. The Supplier shall review and update these security risks at least every 12 months or when there is significant change within the organisation or threat.	Functional	Intersects With	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	
2603	Staff Risk Awareness	The Supplier shall ensure that managers, systems administrators, and users of organisational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organisational information systems. The Supplier shall review and update these security risks at least every 12 months or when there is significant change within the organisation or threat.	Functional	Intersects With	Security, Compliance & Resilience Awareness Training	SAT-02	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	
2603	Staff Risk Awareness	The Supplier shall ensure that managers, systems administrators, and users of organisational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organisational information systems. The Supplier shall review and update these security risks at least every 12 months or when there is significant change within the organisation or threat.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	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	
2604	Acceptable Use Policy	The Supplier's Acceptable Use Policy shall consider and include appropriate enforcement of restrictions on: i) Use of social media, social networking sites, and external sites/applications ii) Posting organisational information on public websites iii) Use of organisation-provided identifiers (e.g. email addresses) and authentication secrets (e.g. passwords) for creating accounts on external sites/applications iv) Enforce clear desk and clear screen requirements v) Handling of physical corporate assets outside the office environment vi) Locations for conducting duties vii) Remote activation of collaborative computing devices viii) Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Functional	Intersects With	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work to enable secure, compliant and resilient capabilities.	8	
2604	Acceptable Use Policy	The Supplier's Acceptable Use Policy shall consider and include appropriate enforcement of restrictions on: i) Use of social media, social networking sites, and external sites/applications ii) Posting organisational information on public websites iii) Use of organisation-provided identifiers (e.g. email addresses) and authentication secrets (e.g. passwords) for creating accounts on external sites/applications iv) Enforce clear desk and clear screen requirements v) Handling of physical corporate assets outside the office environment vi) Locations for conducting duties vii) Remote activation of collaborative computing devices viii) Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Functional	Intersects With	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	8	
2604	Acceptable Use Policy	The Supplier's Acceptable Use Policy shall consider and include appropriate enforcement of restrictions on: i) Use of social media, social networking sites, and external sites/applications ii) Posting organisational information on public websites iii) Use of organisation-provided identifiers (e.g. email addresses) and authentication secrets (e.g. passwords) for creating accounts on external sites/applications iv) Enforce clear desk and clear screen requirements v) Handling of physical corporate assets outside the office environment vi) Locations for conducting duties vii) Remote activation of collaborative computing devices viii) Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Functional	Intersects With	Social Media & Social Networking Restrictions	HRS-05.2	Mechanisms exist to define rules of behavior that contain explicit restrictions on the use of social media and networking sites, posting information on commercial websites and sharing account information.	8	

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
2604	Acceptable Use Policy	The Supplier's Acceptable Use Policy shall consider and include appropriate enforcement of restrictions on: i) Use of social media, social networking sites, and external sites/applications ii) Posting organisational information on public websites iii) Use of organisation-provided identifiers (e.g. email addresses) and authentication secrets (e.g. passwords) for creating accounts on external sites/applications iv) Enforce clear desk and clear screen requirements v) Handling of physical corporate assets outside the office environment vi) Locations for conducting duties vii) Remote activation of collaborative computing devices viii) Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to Technology Assets, Applications and/or Services (TAAS), if used maliciously.	8	
2605	Annual Threat Focused Training Feedback	The Supplier shall conduct practical exercises in awareness training for their organisation that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.	Functional	Intersects With	Simulated Cyber Attack Scenario Training	SAT-02.1	Mechanisms exist to include simulated actual cyber-attacks through practical exercises that are aligned with current threat scenarios.	5	
2605	Annual Threat Focused Training Feedback	The Supplier shall conduct practical exercises in awareness training for their organisation that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.	Functional	Intersects With	Practical Exercises	SAT-03.1	Mechanisms exist to include practical exercises in security, compliance and resilience training that reinforce training objectives.	5	
2700	Personnel Pre-Employment Checks	The Supplier shall, unless prohibited by Applicable Law, perform appropriate background verification checks on Personnel that have access to Data upon hire. The verification checks shall include: i) Verifying credentials ii) Employment history iii) Qualification checks iv) Application or verification of BPSS (Baseline Personnel Security Standard)	Functional	Subset Of	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	
2701	Personnel Security Vetting*	The Supplier shall define and implement a policy for applying BPSS and National Security Vetting (NSV) checks as appropriate for employees that support Functions and the protection of Data. *(It is recognised that application of NSV is normally only possible once a contract requiring such is in place. Potential suppliers who do not meet this requirement at time of submission must, however, be willing and be able to enforce their staff through appropriate levels of vetting within a timescale agreed with the project delivery team following contract award).	Functional	Intersects With	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
2702	Joiners, Movers and Leavers	The Supplier shall define and implement a joiners, movers and leavers policy to secure organisational hardware, software and systems.	Functional	Subset Of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
2702	Joiners, Movers and Leavers	The Supplier shall define and implement a joiners, movers and leavers policy to secure organisational hardware, software and systems.	Functional	Intersects With	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	8	
2702	Joiners, Movers and Leavers	The Supplier shall define and implement a joiners, movers and leavers policy to secure organisational hardware, software and systems.	Functional	Intersects With	User Provisioning & De-Provisioning	IAC-07	Mechanisms exist to utilize a formal user registration and de-registration process that governs the assignment of access rights.	5	
2703	Whistleblowing	The Supplier shall define and implement training and processes for employees and contractors to identify and report suspicious activities and/or behaviour including violations of information security policies and procedures without fear of recrimination. The Supplier shall define and implement a disciplinary process to take action against employees who violate information security policies or procedures.	Functional	Intersects With	Reporting Suspicious Activities	HRS-15	Mechanisms exist to enable personnel to report suspicious activities and/or behavior without fear of reprisal or other negative consequences (e.g., whistleblower protections).	5	
2704	Environmental Controls	The Supplier shall, where appropriate, implement, install, and maintain the following environmental controls supporting Functions and protection of Data: i) Fire suppression systems ii) Temperature and humidity controls within a data centre or server room environment iii) Backup power technology (e.g. uninterruptible power supply, diesel generator, separate grid connection, etc.).	Functional	Intersects With	Fire Suppression Devices	PES-08.2	Facility security mechanisms exist to utilize fire suppression devices/systems that provide automatic notification of any activation to organizational personnel and emergency responders.	8	
2704	Environmental Controls	The Supplier shall, where appropriate, implement, install, and maintain the following environmental controls supporting Functions and protection of Data: i) Fire suppression systems ii) Temperature and humidity controls within a data centre or server room environment iii) Backup power technology (e.g. uninterruptible power supply, diesel generator, separate grid connection, etc.).	Functional	Intersects With	Emergency Power	PES-07.3	Facility security mechanisms exist to supply alternate power, capable of maintaining minimally-required operational capability, in the event of an extended loss of the primary power source.	8	
2704	Environmental Controls	The Supplier shall, where appropriate, implement, install, and maintain the following environmental controls supporting Functions and protection of Data: i) Fire suppression systems ii) Temperature and humidity controls within a data centre or server room environment iii) Backup power technology (e.g. uninterruptible power supply, diesel generator, separate grid connection, etc.).	Functional	Intersects With	Temperature & Humidity Controls	PES-09	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	8	
3100	Security Monitoring	The Supplier shall monitor the security status of the networks and systems supporting the operation of business Functions and protection of Data in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
3102	Continuously Monitor Security Controls	The Supplier shall establish and document security event monitoring which at a minimum covers the following: i) 24x7x365 monitoring of all identified Information Systems in Production and non-Production environments ii) Tools used for 24x7x365 monitoring and correlation iii) Security events covered iv) Frequency of monitoring v) Clearly defined roles and responsibilities vi) Escalation matrix.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
3102	Continuously Monitor Security Controls	The Supplier shall establish and document security event monitoring which at a minimum covers the following: i) 24x7x365 monitoring of all identified Information Systems in Production and non-Production environments ii) Tools used for 24x7x365 monitoring and correlation iii) Security events covered iv) Frequency of monitoring v) Clearly defined roles and responsibilities vi) Escalation matrix.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
3102	Continuously Monitor Security Controls	The Supplier shall establish and document security event monitoring which at a minimum covers the following: i) 24x7x365 monitoring of all identified Information Systems in Production and non-Production environments ii) Tools used for 24x7x365 monitoring and correlation iii) Security events covered iv) Frequency of monitoring v) Clearly defined roles and responsibilities vi) Escalation matrix.	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
3102	Continuously Monitor Security Controls	The Supplier shall establish and document security event monitoring which at a minimum covers the following: i) 24x7x365 monitoring of all identified Information Systems in Production and non-Production environments ii) Tools used for 24x7x365 monitoring and correlation iii) Security events covered iv) Frequency of monitoring v) Clearly defined roles and responsibilities vi) Escalation matrix.	Functional	Subset Of	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.	10	
3102	Continuously Monitor Security Controls	The Supplier shall establish and document security event monitoring which at a minimum covers the following: i) 24x7x365 monitoring of all identified Information Systems in Production and non-Production environments ii) Tools used for 24x7x365 monitoring and correlation iii) Security events covered iv) Frequency of monitoring v) Clearly defined roles and responsibilities vi) Escalation matrix.	Functional	Intersects With	Event Log Review Escalation Matrix	MON-17.1	Mechanisms exist to make event log review processes more efficient and effective by developing and maintaining an incident response escalation matrix.	8	
3103	Securing Logs	The Supplier shall hold logging data securely and grant read access only to accounts with business needs. The Supplier shall protect audit tools from unauthorised access, modification and deletion. Logging data shall be retained and protected from deletion to a documented retention period, after which it shall be 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.	5	
3103	Securing Logs	The Supplier shall hold logging data securely and grant read access only to accounts with business needs. The Supplier shall protect audit tools from unauthorised access, modification and deletion. Logging data shall be retained and protected from deletion to a documented retention period, after which it shall be 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.	5	
3104	Security Event Triage	The Supplier shall provide evidence from their monitoring tool of security incidents to verify the reliability of identified and triggered alerts for triage.	Functional	Intersects With	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5	
3104	Security Event Triage	The Supplier shall provide evidence from their monitoring tool of security incidents to verify the reliability of identified and triggered alerts for triage.	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	
3105	Identifying Security Incidents	The Supplier shall contextualise alerts with knowledge of the threat and their systems, and engage Incident Response when an incident (confirmed or otherwise) is identified.	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	
3105	Identifying Security Incidents	The Supplier shall contextualise alerts with knowledge of the threat and their systems, and engage Incident Response when an incident (confirmed or otherwise) is identified.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
3106	Monitoring Tools and Skills	The Supplier shall ensure that monitoring staff skills, tools and roles, including any that are outsourced, reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have contextual knowledge of the Functions and requirements for the protection of Data.	Functional	Subset Of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring 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	Notes
3106	Monitoring Tools and Skills	The Supplier shall ensure that monitoring staff skills, tools and roles, including any that are outsourced, reflect governance and reporting requirements, expected threats and the complexities of the network or system data they need to use. Monitoring staff have contextual knowledge of the Functions and requirements for the protection of Data.	Functional	Intersects With	Cyber Threat Environment	SAT-03.6	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	
3107	Create, Retain and Correlate Audit Logs	The Supplier shall generate event logs for systems that support the operation of Functions and protection of Data. The following criteria apply: i) Logs are archived for a minimum of 12 months ii) Logs capture (as a minimum) date, time (from a single NTP source), user ID, device accessed and port used iii) Logs capture key security event types (e.g. critical files accessed, user accounts generated, multiple failed login attempts, logging failures from devices, events related to systems that have an internet connection) iv) Access to modify system logs is restricted v) Logs and security event logs can be made available upon request vi) Store audit records in a repository that is part of a physically different system vii) The Supplier shall ensure that systems logs are reviewed at least weekly to identify system failures, faults, or potential security incidents and corrective actions are taken to resolve or address issues within a reasonable timeframe viii) Review, at least every 6 months the event types selected for logging purposes to ensure these still meet business requirements ix) Capture the operational status of the logging system and alert on any failures which impact the system's operational capacity.	Functional	Subset Of	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	10	
3107	Create, Retain and Correlate Audit Logs	The Supplier shall generate event logs for systems that support the operation of Functions and protection of Data. The following criteria apply: i) Logs are archived for a minimum of 12 months ii) Logs capture (as a minimum) date, time (from a single NTP source), user ID, device accessed and port used iii) Logs capture key security event types (e.g. critical files accessed, user accounts generated, multiple failed login attempts, logging failures from devices, events related to systems that have an internet connection) iv) Access to modify system logs is restricted v) Logs and security event logs can be made available upon request vi) Store audit records in a repository that is part of a physically different system vii) The Supplier shall ensure that systems logs are reviewed at least weekly to identify system failures, faults, or potential security incidents and corrective actions are taken to resolve or address issues within a reasonable timeframe viii) Review, at least every 6 months the event types selected for logging purposes to ensure these still meet business requirements ix) Capture the operational status of the logging system and alert on any failures which impact the system's operational capacity.	Functional	Intersects With	Event Log Retention	MON-10	Mechanisms exist to retain event logs for a time period consistent with records retention requirements to provide support for after-the-fact investigations of security incidents and to meet statutory, regulatory and contractual retention requirements.	5	
3108	Audit Reduction and Report Generation	The Supplier shall provide and implement an appropriate audit record reduction and report generation capability that: i) supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and ii) does not alter the original content or time ordering of audit records.	Functional	Intersects With	Monitoring Reporting	MON-06	Mechanisms exist to provide an event log report generation capability to aid in detecting and assessing anomalous activities.	5	
3109	Integration of Records with Incident Management	The Supplier shall integrate audit record review, triage, analysis, and reporting processes with organisational governance and incident management structure.	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	
3110	Monitor Alerts/Advisories and Take Action	The Supplier shall monitor system security alerts and advisories and take action in response.	Functional	Intersects With	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
3110	Monitor Alerts/Advisories and Take Action	The Supplier shall monitor system security alerts and advisories and take action in response.	Functional	Intersects With	Threat Intelligence Reporting	THR-03.1	Mechanisms exist to utilize external threat intelligence feeds to generate and disseminate organization-specific security alerts, advisories and/or directives.	5	
3200	Proactive Security Event Discovery	The Supplier shall detect, within networks and information systems, malicious activity affecting, or with the potential to affect, the operation of business Functions and protection of Data even when the activity evades standard signature-based security prevent/detect solutions (or when standard solutions are not deployable).	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	
3201	System Abnormalities for Attack Detection	The Supplier shall define examples of abnormal system behaviour to aid in detecting malicious activity that is otherwise hard to identify. The Supplier shall take appropriate action upon identifying this behaviour.	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	
3202	Proactive Attack Discovery	The Supplier shall implement reasonable and proportionate measures to detect malicious activity affecting, or with the potential to affect, the operation of Functions and protection of Data.	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	
3203	Use Indicators of Compromise From Alerts	The Supplier shall monitor system security alerts and advisories and take action in response using agreed and managed indicators of compromise.	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	
3204	Presence of Unauthorised System Components	The Supplier shall implement proportionate measures to: i) Detect the presence of unauthorised hardware, software, and firmware components within the system using tooling ii) Take the following actions when unauthorised components are detected: disable network access by such components; isolate the components; notify systems administrators and/or security operations teams.	Functional	Intersects With	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	8	
4100	Response and Recovery Planning	The Supplier shall implement well-defined and tested incident management processes that aim to ensure continuity of business Functions and protection of Data in the event of system or service failure. Mitigation activities are designed and where possible automated to contain or limit the impact of a compromise.	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	
4101	Response Plan	The Supplier shall have an up-to-date incident response plan that is grounded in a thorough risk assessment that takes account of business Functions and protection of Data and covers a range of incident scenarios.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
4102	Response and Recovery Capability	The Supplier shall have the capability to enact their incident response plan, including effective limitation of impact on the operation of Functions and protection of Data. During an incident, the Supplier shall enact processes and capabilities to provide access to information sources on which to base their response decisions to coordinate incident handling activities with contingency planning activities.	Functional	Intersects With	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
4103	Testing and Exercising	The Supplier shall carry out exercises to test response plans at least every 12 months, using past incidents that affected their (and other's) organisation, and scenarios that draw on threat intelligence and risk assessments.	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.	5	
4104	Incident Handling Capability	The Supplier shall establish an operational incident handling capability for organisational information systems that is consistently applied across the organisation and includes: i) Adequate preparation, detection, forensic analysis, containment, recovery, and user response activities ii) Tracking, documenting, and reporting incidents to appropriate organisational officials and/or authorities iii) Sufficient rigour, intensity and scope.	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	
4104	Incident Handling Capability	The Supplier shall establish an operational incident handling capability for organisational information systems that is consistently applied across the organisation and includes: i) Adequate preparation, detection, forensic analysis, containment, recovery, and user response activities ii) Tracking, documenting, and reporting incidents to appropriate organisational officials and/or authorities iii) Sufficient rigour, intensity and scope.	Functional	Intersects With	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
4105	Exfiltration Tests	The Supplier shall conduct data exfiltration tests at the network boundaries at least every 12 months. These tests must be conducted against both authorised and covert channels.	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.	3	
4106	Attempted Unauthorised Connections From Staff	The Supplier shall audit the identity of internal users associated with denied communications.	Functional	Intersects With	Unauthorized Activities	MON-16.3	Mechanisms exist to monitor for unauthorized activities, accounts, connections, devices and software.	5	
4200	Lessons Learned	The Supplier shall, when an incident occurs, incorporate root cause analysis and lessons learned information from incident response activities into incident response procedures, training and testing. The Supplier shall implement the resulting improvements immediately or, at minimum, within 30 days of the completion of the root cause analysis.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity and data protection incidents to reduce the likelihood or impact of future incidents.	5	
4201	Business Continuity Risk Assessments	The Supplier shall perform Business Continuity Risk Assessments to determine relevant risks, threats, and likelihood & impact of a service outage or Data Breach. The Supplier shall record the output of these Risk Assessments within a risk register along with the required controls and/or procedures to mitigate or remove the risk and/or threat.	Functional	Intersects With	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess security, compliance and resilience risks.	5	
4201	Business Continuity Risk Assessments	The Supplier shall perform Business Continuity Risk Assessments to determine relevant risks, threats, and likelihood & impact of a service outage or Data Breach. The Supplier shall record the output of these Risk Assessments within a risk register along with the required controls and/or procedures to mitigate or remove the risk and/or threat.	Functional	Intersects With	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
4202	Operation Resilience For Equipment	The Supplier shall assess the requirement for redundant networking and telecommunication systems to protect Functions and Data. Where required, the Supplier shall implement and protect these systems.	Functional	Intersects With	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
4202	Operation Resilience For Equipment	The Supplier shall assess the requirement for redundant networking and telecommunication systems to protect Functions and Data. Where required, the Supplier shall implement and protect these systems.	Functional	Intersects With	Failover Capability	BCD-12.2	Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical Technology Assets, Applications, Services and/or Data (TAASD).	5	