NIST IR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document : Secure Controls Framework (SCF) version 2025.2
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document: **NIS2 Directive Annex**
Focal Document URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=intcom:C%282024%297151
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
1	POLICY ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS (ARTICLE 21(2), POINT (A) OF DIRECTIVE (EU) 2022/2555)	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
1.1	Policy on the security of network and information systems	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
1.1.1	N/A	For the purpose of Article 21(2), point (a) of Directive (EU) 2022/2555, the policy on the security of network and information systems shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
1.1.1(a)	N/A	set out the relevant entities' approach to managing the security of their network and information systems;	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
1.1.1(a)	N/A	set out the relevant entities' approach to managing the security of their network and information systems;	Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
1.1.1(b)	N/A	be appropriate to and complementary with the relevant entities' business strategy and objectives;	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
1.1.1(b)	N/A	be appropriate to and complementary with the relevant entities' business strategy and objectives;	Functional	intersects with	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	8	
1.1.1(c)	N/A	set out network and information security objectives;	Functional	equal	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	10	
1.1.1(d)	N/A	include a commitment to continual improvement of the security of network and information systems;	Functional	subset of	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's cybersecurity & data privacy program, including appropriate: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	10	
1.1.1(e)	N/A	include a commitment to provide the appropriate resources needed for its implementation, including the necessary staff, financial resources, processes, tools and technologies;	Functional	subset of	Commitment To Continual Improvements	GOV-01.3	Mechanisms exist to commit appropriate resources needed for continual improvement of the organization's cybersecurity & data privacy program, including appropriate: (1) Staffing; (2) Budget; (3) Processes; and (4) Technologies.	10	
1.1.1(f)	N/A	be communicated to and acknowledged by relevant employees and relevant interested external parties;	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	8	
1.1.1(f)	N/A	be communicated to and acknowledged by relevant employees and relevant interested external parties;	Functional	intersects with	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's cybersecurity & data privacy policies and provide acknowledgement.	8	
1.1.1(g)	N/A	lay down roles and responsibilities pursuant to point 1.2.;	Functional	subset of	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	10	
1.1.1(g)	N/A	lay down roles and responsibilities pursuant to point 1.2.;	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
1.1.1(h)	N/A	list the documentation to be kept and the duration of retention of the documentation;	Functional	subset of	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	10	
1.1.1(i)	N/A	list the topic-specific policies;	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
1.1.1(j)	N/A	lay down indicators and measures to monitor its implementation and the current status of relevant entities' maturity level of network and information security;	Functional	subset of	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	10	
1.1.1(k)	N/A	indicate the date of the formal approval by the management bodies of the relevant entities (the 'management bodies').	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	8	
1.1.1(k)	N/A	indicate the date of the formal approval by the management bodies of the relevant entities (the 'management bodies').	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
1.1.2	N/A	The network and information system security policy shall be reviewed and, where appropriate, updated by management bodies at least annually and when significant incidents or significant changes to operations or risks occur. The result of the reviews shall be documented.	Functional	subset of	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	10	
1.2	Roles, responsibilities and authorities	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
1.2.1	N/A	As part of their policy on the security of network and information systems referred to in point 1.1., the relevant entities shall lay down responsibilities and authorities for network and information system security and assign them to roles, allocate them according to the relevant entities' needs, and communicate them to the management bodies.	Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	8	
1.2.1	N/A	As part of their policy on the security of network and information systems referred to in point 1.1., the relevant entities shall lay down responsibilities and authorities for network and information system security and assign them to roles, allocate them according to the relevant entities' needs, and communicate them to the management bodies.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
1.2.2	N/A	The relevant entities shall require all personnel and third parties to apply network and information system security in accordance with the established network and information security policy, topic-specific policies and procedures of the relevant entities.	Functional	intersects with	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity & data privacy principles in their daily work.	5	
1.2.2	N/A	The relevant entities shall require all personnel and third parties to apply network and information system security in accordance with the established network and information security policy, topic-specific policies and procedures of the relevant entities.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
1.2.3	N/A	At least one person shall report directly to the management bodies on matters of network and information system security.	Functional	subset of	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	10	
1.2.3	N/A	At least one person shall report directly to the management bodies on matters of network and information system security.	Functional	intersects with	Cybersecurity & Data Privacy Status Reporting	GOV-17	Mechanisms exist to submit status reporting of the organization's cybersecurity and/or data privacy program to applicable statutory and/or regulatory authorities, as required.	5	
1.2.4	N/A	Depending on the size of the relevant entities, network and information system security shall be covered by dedicated roles or duties carried out in addition to existing roles.	Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	8	
1.2.4	N/A	Depending on the size of the relevant entities, network and information system security shall be covered by dedicated roles or duties carried out in addition to existing roles.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
1.2.5	N/A	Conflicting duties and conflicting areas of responsibility shall be segregated, where applicable.	Functional	subset of	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	10	
1.2.6	N/A	Roles, responsibilities and authorities shall be reviewed and, where appropriate, updated by management bodies at planned intervals and when significant incidents or significant changes to operations or risks occur.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	8	
1.2.6	N/A	Roles, responsibilities and authorities shall be reviewed and, where appropriate, updated by management bodies at planned intervals and when significant incidents or significant changes to operations or risks occur.	Functional	intersects with	Change of Roles & Duties	IAC-07.1	Mechanisms exist to revoke user access rights following changes in personnel roles and duties, if no longer necessary or permitted.	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 (optional)	Notes (optional)
2	RISK MANAGEMENT POLICY (ARTICLE 21(2), POINT (A) OF DIRECTIVE (EU) 2022/2555)	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
2.1	Risk management framework	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
2.1.1	N/A	For the purpose of Article 21(2), point (a) of Directive (EU) 2022/2555, the relevant entities shall establish and maintain an appropriate risk management framework to identify and address the risks posed to the security of network and information systems. The relevant entities shall perform and document risk assessments and, based on the results, establish, implement and monitor a risk treatment plan. Risk assessment results and residual risks shall be accepted by management bodies or, where applicable, by persons who are accountable and have the authority to manage risks, provided that the relevant entities ensure adequate reporting to the management bodies.	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
2.1.1	N/A	For the purpose of Article 21(2), point (a) of Directive (EU) 2022/2555, the relevant entities shall establish and maintain an appropriate risk management framework to identify and address the risks posed to the security of network and information systems. The relevant entities shall perform and document risk assessments and, based on the results, establish, implement and monitor a risk treatment plan. Risk assessment results and residual risks shall be accepted by management bodies or, where applicable, by persons who are accountable and have the authority to manage risks, provided that the relevant entities ensure adequate reporting to the management bodies.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
2.1.1	N/A	For the purpose of Article 21(2), point (a) of Directive (EU) 2022/2555, the relevant entities shall establish and maintain an appropriate risk management framework to identify and address the risks posed to the security of network and information systems. The relevant entities shall perform and document risk assessments and, based on the results, establish, implement and monitor a risk treatment plan. Risk assessment results and residual risks shall be accepted by management bodies or, where applicable, by persons who are accountable and have the authority to manage risks, provided that the relevant entities ensure adequate reporting to the management bodies.	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 systems and data.	5	
2.1.1	N/A	For the purpose of Article 21(2), point (a) of Directive (EU) 2022/2555, the relevant entities shall establish and maintain an appropriate risk management framework to identify and address the risks posed to the security of network and information systems. The relevant entities shall perform and document risk assessments and, based on the results, establish, implement and monitor a risk treatment plan. Risk assessment results and residual risks shall be accepted by management bodies or, where applicable, by persons who are accountable and have the authority to manage risks, provided that the relevant entities ensure adequate reporting to the management bodies.	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
2.1.2	N/A	For the purpose of point 2.1.1., the relevant entities shall establish procedures for identification, analysis, assessment and treatment of risks (‘cybersecurity risk management process’). The cybersecurity risk management process shall be an integral part of the relevant entities’ overall risk management process, where applicable. As part of the cybersecurity risk management process, the relevant entities shall:	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
2.1.2	N/A	For the purpose of point 2.1.1., the relevant entities shall establish procedures for identification, analysis, assessment and treatment of risks (‘cybersecurity risk management process’). The cybersecurity risk management process shall be an integral part of the relevant entities’ overall risk management process, where applicable. As part of the cybersecurity risk management process, the relevant entities shall:	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	8	
2.1.2	N/A	For the purpose of point 2.1.1., the relevant entities shall establish procedures for identification, analysis, assessment and treatment of risks (‘cybersecurity risk management process’). The cybersecurity risk management process shall be an integral part of the relevant entities’ overall risk management process, where applicable. As part of the cybersecurity risk management process, the relevant entities shall:	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 systems and data.	8	
2.1.2	N/A	For the purpose of point 2.1.1., the relevant entities shall establish procedures for identification, analysis, assessment and treatment of risks (‘cybersecurity risk management process’). The cybersecurity risk management process shall be an integral part of the relevant entities’ overall risk management process, where applicable. As part of the cybersecurity risk management process, the relevant entities shall:	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	8	
2.1.2(a)	N/A	follow a risk management methodology;	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
2.1.2(b)	N/A	establish the risk tolerance level in accordance with the risk appetite of the relevant entities;	Functional	intersects with	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	8	
2.1.2(b)	N/A	establish the risk tolerance level in accordance with the risk appetite of the relevant entities;	Functional	intersects with	Risk Appetite	RSK-01.5	Mechanisms exist to define organizational risk appetite, the degree of uncertainty the organization is willing to accept in anticipation of a reward.	8	
2.1.2(c)	N/A	establish and maintain relevant risk criteria;	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
2.1.2(c)	N/A	establish and maintain relevant risk criteria;	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	8	
2.1.2(d)	N/A	in line with an all-hazards approach, identify and document the risks posed to the security of network and information systems, in particular in relation to third parties and risks that could lead to disruptions in the availability, integrity, authenticity and confidentiality of the network and information systems, including the identification of single point of failures;	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
2.1.2(d)	N/A	in line with an all-hazards approach, identify and document the risks posed to the security of network and information systems, in particular in relation to third parties and risks that could lead to disruptions in the availability, integrity, authenticity and confidentiality of the network and information systems, including the identification of single point of failures;	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	8	
2.1.2(d)	N/A	in line with an all-hazards approach, identify and document the risks posed to the security of network and information systems, in particular in relation to third parties and risks that could lead to disruptions in the availability, integrity, authenticity and confidentiality of the network and information systems, including the identification of single point of failures;	Functional	intersects with	Risk Catalog	RSK-03.1	Mechanisms exist to develop and keep current a catalog of applicable risks associated with the organization's business operations and technologies in use.	8	
2.1.2(d)	N/A	in line with an all-hazards approach, identify and document the risks posed to the security of network and information systems, in particular in relation to third parties and risks that could lead to disruptions in the availability, integrity, authenticity and confidentiality of the network and information systems, including the identification of single point of failures;	Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	8	
2.1.2(e)	N/A	analyse the risks posed to the security of network and information systems, including threat, likelihood, impact, and risk level, taking into account cyber threat intelligence and vulnerabilities;	Functional	intersects with	Risk Management Resourcing	RSK-01.2	Mechanisms exist to reduce the magnitude or likelihood of potential impacts by resourcing the capability required to manage technology-related risks.	5	
2.1.2(e)	N/A	analyse the risks posed to the security of network and information systems, including threat, likelihood, impact, and risk level, taking into account cyber threat intelligence and vulnerabilities;	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 systems and data.	5	
2.1.2(e)	N/A	analyse the risks posed to the security of network and information systems, including threat, likelihood, impact, and risk level, taking into account cyber threat intelligence and vulnerabilities;	Functional	intersects with	Risk Ranking	RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
2.1.2(f)	N/A	evaluate the identified risks based on the risk criteria;	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 systems and data.	8	
2.1.2(g)	N/A	identify and prioritise appropriate risk treatment options and measures;	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
2.1.2(h)	N/A	continuously monitor the implementation of the risk treatment measures;	Functional	intersects with	Risk Monitoring	RSK-11	Mechanisms exist to ensure risk monitoring as an integral part of the continuous monitoring strategy that includes monitoring the effectiveness of cybersecurity & data privacy controls, compliance and change management.	5	
2.1.2(i)	N/A	identify who is responsible for implementing the risk treatment measures and when they should be implemented;	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
2.1.2(j)	N/A	document the chosen risk treatment measures in a risk treatment plan and the reasons justifying the acceptance of residual risks in a comprehensible manner.	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
2.1.3	N/A	When identifying and prioritising appropriate risk treatment options and measures, the relevant entities shall take into account the risk assessment results, the results of the procedure to assess the effectiveness of cybersecurity risk-management measures, the cost of implementation in relation to the expected benefit, the asset classification referred to in point 12.1., and the business impact analysis referred to in point 4.1.3.	Functional	intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
2.1.3	N/A	When identifying and prioritising appropriate risk treatment options and measures, the relevant entities shall take into account the risk assessment results, the results of the procedure to assess the effectiveness of cybersecurity risk-management measures, the cost of implementation in relation to the expected benefit, the asset classification referred to in point 12.1., and the business impact analysis referred to in point 4.1.3.	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 systems and data.	5	
2.1.3	N/A	When identifying and prioritising appropriate risk treatment options and measures, the relevant entities shall take into account the risk assessment results, the results of the procedure to assess the effectiveness of cybersecurity risk-management measures, the cost of implementation in relation to the expected benefit, the asset classification referred to in point 12.1., and the business impact analysis referred to in point 4.1.3.	Functional	intersects with	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	8	
2.1.3	N/A	When identifying and prioritising appropriate risk treatment options and measures, the relevant entities shall take into account the risk assessment results, the results of the procedure to assess the effectiveness of cybersecurity risk-management measures, the cost of implementation in relation to the expected benefit, the asset classification referred to in point 12.1., and the business impact analysis referred to in point 4.1.3.	Functional	intersects with	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	5	
2.1.4	N/A	The relevant entities shall review and, where appropriate, update the risk assessment results and the risk treatment plan at planned intervals and at least annually, and when significant changes to operations or risks or significant incidents occur.	Functional	intersects with	Risk Assessment Update	RSK-07	Mechanisms exist to routinely update risk assessments and react accordingly upon identifying new security vulnerabilities, including using outside sources for security vulnerability information.	5	
2.2	RISK MANAGEMENT POLICY (ARTICLE 21(2), POINT (A) OF DIRECTIVE (EU) 2022/2555)	Compliance monitoring	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
2.2.1	N/A	The relevant entities shall regularly review the compliance with their policies on network and information system security, topic-specific policies, rules, and standards. The management bodies shall be informed of the status of network and information security on the basis of the compliance reviews by means of regular reporting.	Functional	intersects with	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	8	
2.2.1	N/A	The relevant entities shall regularly review the compliance with their policies on network and information system security, topic-specific policies, rules, and standards. The management bodies shall be informed of the status of network and information security on the basis of the compliance reviews by means of regular reporting.	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
2.2.2	N/A	The relevant entities shall put in place an effective compliance reporting system which shall be appropriate to their structures, operating environments and threat landscapes. The compliance reporting system shall be capable to provide to the management bodies an informed view of the current state of the relevant entities' management of risks.	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
2.2.3	N/A	The relevant entities shall perform the compliance monitoring at planned intervals and when significant incidents or significant changes to operations or risks occur.	Functional	intersects with	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	5	
2.2.3	N/A	The relevant entities shall perform the compliance monitoring at planned intervals and when significant incidents or significant changes to operations or risks occur.	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
2.3	RISK MANAGEMENT POLICY (ARTICLE 21(2), POINT (A) OF DIRECTIVE (EU) 2022/2555)	Independent review of information and network security	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
2.3.1	N/A	The relevant entities shall review independently their approach to managing network and information system security and its implementation including people, processes and technologies.	Functional	intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
2.3.1	N/A	The relevant entities shall review independently their approach to managing network and information system security and its implementation including people, processes and technologies.	Functional	intersects with	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate cybersecurity & data protection controls at planned intervals or when the system, service or project undergoes significant changes.	5	
2.3.2	N/A	The relevant entities shall develop and maintain processes to conduct independent reviews which shall be carried out by individuals with appropriate audit competence. Where the independent review is conducted by staff members of the relevant entity, the persons conducting the reviews shall not be in the line of authority of the personnel of the area under review. If the size of the relevant entities does not allow such separation of line of authority, the relevant entities shall put in place alternative measures to guarantee the impartiality of the reviews.	Functional	subset of	Internal Audit Function	CPL-02.1	Mechanisms exist to implement an internal audit function that is capable of providing senior organization management with insights into the appropriateness of the organization's technology and information governance processes.	10	
2.3.2	N/A	The relevant entities shall develop and maintain processes to conduct independent reviews which shall be carried out by individuals with appropriate audit competence. Where the independent review is conducted by staff members of the relevant entity, the persons conducting the reviews shall not be in the line of authority of the personnel of the area under review. If the size of the relevant entities does not allow such separation of line of authority, the relevant entities shall put in place alternative measures to guarantee the impartiality of the reviews.	Functional	intersects with	Periodic Audits	CPL-02.2	Mechanisms exist to conduct periodic audits of cybersecurity & data protection controls to evaluate conformity with the organization's documented policies, standards and procedures.	8	
2.3.3	N/A	The results of the independent reviews, including the results from the compliance monitoring pursuant to point 2.2. and the monitoring and measurement pursuant to point 7, shall be reported to the management bodies. Corrective actions shall be taken or residual risk accepted according to the relevant entities' risk acceptance criteria.	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
2.3.4	N/A	The independent reviews shall take place at planned intervals and when significant incidents or significant changes to operations or risks occur.	Functional	intersects with	Periodic Audits	CPL-02.2	Mechanisms exist to conduct periodic audits of cybersecurity & data protection controls to evaluate conformity with the organization's documented policies, standards and procedures.	5	
3	INCIDENT HANDLING (ARTICLE 21(2), POINT (B), OF DIRECTIVE (EU) 2022/2555)	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
3.1	Incident handling policy	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
3.1.1	N/A	For the purpose of Article 21(2), point (b) of Directive (EU) 2022/2555, the relevant entities shall establish and implement an incident handling policy laying down the roles, responsibilities, and procedures for detecting, analysing, containing or responding to, recovering from, documenting and reporting of incidents in a timely manner.	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 & data privacy-related incidents.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.1.1	N/A	For the purpose of Article 21(2), point (b) of Directive (EU) 2022/2555, the relevant entities shall establish and implement an incident handling policy laying down the roles, responsibilities, and procedures for detecting, analysing, containing or responding to, recovering from, documenting and reporting of incidents in a timely manner.	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	
3.1.2	N/A	The policy referred to in point 3.1.1 shall be coherent with the business continuity and disaster recovery plan referred to in point 4.1. The policy shall include:	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
3.1.2(a)	N/A	a categorisation system for incidents that is consistent with the event assessment and classification carried out pursuant to point 3.4.1.;	Functional	intersects with	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5	
3.1.2(b)	N/A	effective communication plans including for escalation and reporting;	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	
3.1.2(b)	N/A	effective communication plans including for escalation and reporting;	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	
3.1.2(b)	N/A	effective communication plans including for escalation and reporting;	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
3.1.2(b)	N/A	effective communication plans including for escalation and reporting;	Functional	intersects with	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
3.1.2(c)	N/A	assignment of roles to detect and appropriately respond to incidents to competent employees;	Functional	subset of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
3.1.2(c)	N/A	assignment of roles to detect and appropriately respond to incidents to competent employees;	Functional	intersects with	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
3.1.2(d)	N/A	documents to be used in the course of incident detection and response such as incident response manuals, escalation charts, contact lists and templates.	Functional	subset of	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	10	
3.1.3	N/A	The roles, responsibilities and procedures laid down in the policy shall be tested and reviewed and, where appropriate, updated at planned intervals and after significant incidents or significant changes to operations or risks.	Functional	subset of	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
3.1.3	N/A	The roles, responsibilities and procedures laid down in the policy shall be tested and reviewed and, where appropriate, updated at planned intervals and after significant incidents or significant changes to operations or risks.	Functional	intersects with	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
3.2	Monitoring and logging	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
3.2.1	N/A	The relevant entities shall lay down procedures and use tools to monitor and log activities on their network and information systems to detect events that could be considered as incidents and respond accordingly to mitigate the impact.	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 & data privacy-related incidents.	10	
3.2.1	N/A	The relevant entities shall lay down procedures and use tools to monitor and log activities on their network and information systems to detect events that could be considered as incidents and respond accordingly to mitigate the impact.	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
3.2.2	N/A	To the extent feasible, monitoring shall be automated and carried out either continuously or in periodic intervals, subject to business capabilities. The relevant entities shall implement their monitoring activities in a way which minimises false positives and false negatives.	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
3.2.2	N/A	To the extent feasible, monitoring shall be automated and carried out either continuously or in periodic intervals, subject to business capabilities. The relevant entities shall implement their monitoring activities in a way which minimises false positives and false negatives.	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	
3.2.3	N/A	Based on the procedures referred to in point 3.2.1., the relevant entities shall maintain, document, and review logs. The relevant entities shall establish a list of assets to be subject to logging based on the results of the risk assessment carried out pursuant to point 2.1. Where appropriate, logs shall include:	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	
3.2.3	N/A	Based on the procedures referred to in point 3.2.1., the relevant entities shall maintain, document, and review logs. The relevant entities shall establish a list of assets to be subject to logging based on the results of the risk assessment carried out pursuant to point 2.1. Where appropriate, logs shall include:	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.	3	
3.2.3	N/A	Based on the procedures referred to in point 3.2.1., the relevant entities shall maintain, document, and review logs. The relevant entities shall establish a list of assets to be subject to logging based on the results of the risk assessment carried out pursuant to point 2.1. Where appropriate, logs shall include:	Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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.	8	
3.2.3(a)	N/A	relevant outbound and inbound network traffic;	Functional	intersects with	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	
3.2.3(b)	N/A	creation, modification or deletion of users of the relevant entities' network and information systems and extension of the permissions;	Functional	intersects with	Account Creation and Modification Logging	MON-16.4	Automated mechanisms exist to generate event logs for permissions changes to privileged accounts and/or groups.	5	
3.2.3(c)	N/A	access to systems and applications;	Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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.	8	
3.2.3(d)	N/A	authentication-related events;	Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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	
3.2.3(e)	N/A	all privileged access to systems and applications, and activities performed by administrative accounts;	Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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	
3.2.3(f)	N/A	access or changes to critical configuration and backup files;	Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.2.3(g)	N/A	event logs and logs from security tools, such as antivirus, intrusion detection systems or firewalls;	Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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	
3.2.3(h)	N/A	use of system resources, as well as their performance;	Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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	
3.2.3(i)	N/A	physical access to facilities;	Functional	intersects with	Correlation with Physical Monitoring	MON-02.4	Automated mechanisms exist to correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual or malevolent activity.	5	
3.2.3(j)	N/A	access to and use of their network equipment and devices;	Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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	
3.2.3(k)	N/A	activation, stopping and pausing of the various logs;	Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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	
3.2.3(l)	N/A	environmental events.	Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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.	3	
3.2.4	N/A	The logs shall be regularly reviewed for any unusual or unwanted trends. Where appropriate, the relevant entities shall lay down appropriate values for alarm thresholds. If the laid down values for alarm threshold are exceeded, an alarm shall be triggered, where appropriate, automatically. The relevant entities shall ensure that, in case of an alarm, a qualified and appropriate response is initiated in a timely manner.	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	
3.2.5	N/A	The relevant entities shall maintain and back up logs for a predefined period and shall protect them from unauthorised access or changes.	Functional	subset of	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.	10	
3.2.6	N/A	To the extent feasible, the relevant entities shall ensure that all systems have synchronised time sources to be able to correlate logs between systems for event assessment. The relevant entities shall establish and keep a list of all assets that are being logged and ensure that monitoring and logging systems are redundant. The availability of the monitoring and logging systems shall be monitored independent of the systems they are monitoring.	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
3.2.6	N/A	To the extent feasible, the relevant entities shall ensure that all systems have synchronised time sources to be able to correlate logs between systems for event assessment. The relevant entities shall establish and keep a list of all assets that are being logged and ensure that monitoring and logging systems are redundant. The availability of the monitoring and logging systems shall be monitored independent of the systems they are monitoring.	Functional	intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support the centralized collection of security-related event logs.	5	
3.2.6	N/A	To the extent feasible, the relevant entities shall ensure that all systems have synchronised time sources to be able to correlate logs between systems for event assessment. The relevant entities shall establish and keep a list of all assets that are being logged and ensure that monitoring and logging systems are redundant. The availability of the monitoring and logging systems shall be monitored independent of the systems they are monitoring.	Functional	intersects with	Inventory of Technology Asset Event Logging	MON-02.9	Mechanisms exist to maintain a current and accurate inventory of technology assets being logged.	5	
3.2.6	N/A	To the extent feasible, the relevant entities shall ensure that all systems have synchronised time sources to be able to correlate logs between systems for event assessment. The relevant entities shall establish and keep a list of all assets that are being logged and ensure that monitoring and logging systems are redundant. The availability of the monitoring and logging systems shall be monitored independent of the systems they are monitoring.	Functional	intersects with	Synchronization With Authoritative Time Source	MON-07.1	Mechanisms exist to synchronize internal system clocks with an authoritative time source.	5	
3.2.7	N/A	The procedures as well as the list of assets that are being logged shall be reviewed and, where appropriate, updated at regular intervals and after significant incidents.	Functional	intersects with	Inventory of Technology Asset Event Logging	MON-02.9	Mechanisms exist to maintain a current and accurate inventory of technology assets being logged.	8	
3.3	Event reporting	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
3.3.1	N/A	The relevant entities shall put in place a simple mechanism allowing their employees, suppliers, and customers to report suspicious events.	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	
3.3.1	N/A	The relevant entities shall put in place a simple mechanism allowing their employees, suppliers, and customers to report suspicious events.	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	
3.3.2	N/A	The relevant entities shall, where appropriate, communicate the event reporting mechanism to their suppliers and customers, and shall regularly train their employees how to use the mechanism.	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	
3.3.2	N/A	The relevant entities shall, where appropriate, communicate the event reporting mechanism to their suppliers and customers, and shall regularly train their employees how to use the mechanism.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
3.4	Event assessment and classification	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
3.4.1	N/A	The relevant entities shall assess suspicious events to determine whether they constitute incidents and, if so, determine their nature and severity.	Functional	subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
3.4.1	N/A	The relevant entities shall assess suspicious events to determine whether they constitute incidents and, if so, determine their nature and severity.	Functional	intersects with	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5	
3.4.2	N/A	For the purpose of point 3.4.1, the relevant entities shall act in the following manner:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
3.4.2(a)	N/A	carry out the assessment based on predefined criteria laid down in advance, and on a triage to determine prioritisation of incident containment and eradication;	Functional	intersects with	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	8	
3.4.2(b)	N/A	assess the existence of recurring incidents as referred to in Article 4 of this Regulation on a quarterly basis;	Functional	intersects with	Recurring Incident Analysis	IRO-09.2	Mechanisms exist to periodically review incident response activities for the existence of recurring incidents.	5	
3.4.2(c)	N/A	review the appropriate logs for the purposes of event assessment and classification;	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.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
3.4.2(d)	N/A	put in place a process for log correlation and analysis, and	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.	5	
3.4.2(e)	N/A	reassess and reclassify events in case of new information becoming available or after analysis of previously available information.	Functional	subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
3.5	Incident response	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
3.5.1	N/A	The relevant entities shall respond to incidents in accordance with documented procedures and in a timely manner.	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 & data privacy-related incidents.	10	
3.5.1	N/A	The relevant entities shall respond to incidents in accordance with documented procedures and in a timely manner.	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	
3.5.2	N/A	The incident response procedures shall include the following stages:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
3.5.2(a)	N/A	incident containment, to prevent the consequences of the incident from spreading;	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	
3.5.2(b)	N/A	eradication, to prevent the incident from continuing or reappearing,	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	
3.5.2(c)	N/A	recovery from the incident, where necessary.	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	
3.5.3	N/A	The relevant entities shall establish communication plans and procedures:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
3.5.3(a)	N/A	with the Computer Security Incident Response Teams (CSIRTs) or, where applicable, the competent authorities, related to incident notification;	Functional	intersects with	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
3.5.3(b)	N/A	for communication among staff members of the relevant entity, and for communication with relevant stakeholders external to the relevant entity.	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	
3.5.3(b)	N/A	for communication among staff members of the relevant entity, and for communication with relevant stakeholders external to the relevant entity.	Functional	intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	5	
3.5.4	N/A	The relevant entities shall log incident response activities in accordance with the procedures referred to in point 3.2.1., and record evidence.	Functional	subset of	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	10	
3.5.5	N/A	The relevant entities shall test at planned intervals their incident response procedures.	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	
3.6	Post-incident reviews	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
3.6.1	N/A	Where appropriate, the relevant entities shall carry out post-incident reviews after recovery from incidents. The post-incident reviews shall identify, where possible, the root cause of the incident and result in documented lessons learned to reduce the occurrence and consequences of future incidents.	Functional	subset of	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	10	
3.6.2	N/A	The relevant entities shall ensure that post-incident reviews contribute to improving their approach to network and information security, to risk treatment measures, and to incident handling, detection and response procedures.	Functional	subset of	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	10	
3.6.3	N/A	The relevant entities shall review at planned intervals if incidents led to post-incident reviews.	Functional	subset of	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	10	
4	BUSINESS CONTINUITY AND CRISIS MANAGEMENT (ARTICLE 21(2), POINT (C), OF DIRECTIVE (EU) 2022/2555)	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
4.1	Business continuity and disaster recovery plan	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
4.1.1	N/A	For the purpose of Article 21(2), point (c) of Directive (EU) 2022/2555, the relevant entities shall lay down and maintain a business continuity and disaster recovery plan to apply in the case of incidents.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
4.1.2	N/A	The relevant entities' operations shall be restored according to the business continuity and disaster recovery plan. The plan shall be based on the results of the risk assessment carried out pursuant to point 2.1 and shall include, where appropriate, the following:	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
4.1.2(a)	N/A	purpose, scope and audience;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
4.1.2(b)	N/A	roles and responsibilities;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
4.1.2(c)	N/A	key contacts and (internal and external) communication channels;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
4.1.2(c)	N/A	key contacts and (internal and external) communication channels;	Functional	intersects with	Recovery Operations Communications	BCD-01.6	Mechanisms exist to communicate the status of recovery activities and progress in restoring operational capabilities to designated internal and external stakeholders.	5	
4.1.2(d)	N/A	conditions for plan activation and deactivation;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
4.1.2(e)	N/A	order of recovery for operations;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
4.1.2(f)	N/A	recovery plans for specific operations, including recovery objectives;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
4.1.2(f)	N/A	recovery plans for specific operations, including recovery objectives;	Functional	intersects with	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
4.1.2(g)	N/A	required resources, including backups and redundancies;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
4.1.2(g)	N/A	required resources, including backups and redundancies;	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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
4.1.2(g)	N/A	required resources, including backups and redundancies;	Functional	intersects with	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover system, which is not collocated with the primary system, application and/or service, which can be activated with little-to-no loss of information or disruption to operations.	5	
4.1.2(h)	N/A	restoring and resuming activities from temporary measures.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
4.1.2(h)	N/A	restoring and resuming activities from temporary measures.	Functional	intersects with	Resume All Missions & Business Functions	BCD-02.1	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.	5	
4.1.2(h)	N/A	restoring and resuming activities from temporary measures.	Functional	intersects with	Resume Essential Missions & Business Functions	BCD-02.3	Mechanisms exist to resume essential missions and business functions within an organization-defined time period of contingency plan activation.	5	
4.1.3	N/A	The relevant entities shall carry out a business impact analysis to assess the potential impact of severe disruptions to their business operations and shall, based on the results of the business impact analysis, establish continuity requirements for the network and information systems.	Functional	intersects with	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	5	
4.1.4	N/A	The business continuity plan and disaster recovery plan shall be tested, reviewed and, where appropriate, updated at planned intervals and following significant incidents or significant changes to operations or risks. The relevant entities shall ensure that the plans incorporate lessons learnt from such tests.	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	
4.1.4	N/A	The business continuity plan and disaster recovery plan shall be tested, reviewed and, where appropriate, updated at planned intervals and following significant incidents or significant changes to operations or risks. The relevant entities shall ensure that the plans incorporate lessons learnt from such tests.	Functional	intersects with	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	
4.2	Backup and redundancy management	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
4.2.1	N/A	The relevant entities shall maintain backup copies of data and provide sufficient available resources, including facilities, network and information systems and staff, to ensure an appropriate level of redundancy.	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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	8	
4.2.1	N/A	The relevant entities shall maintain backup copies of data and provide sufficient available resources, including facilities, network and information systems and staff, to ensure an appropriate level of redundancy.	Functional	intersects with	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover system, which is not collocated with the primary system, application and/or service, which can be activated with little-to-no loss of information or disruption to operations.	5	
4.2.2	N/A	Based on the results of the risk assessment carried out pursuant to point 2.1 and the business continuity plan, the relevant entities shall lay down backup plans which include the following:	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
4.2.2(a)	N/A	recovery times;	Functional	intersects with	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
4.2.2(b)	N/A	assurance that backup copies are complete and accurate, including configuration data and data stored in cloud computing service environment;	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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
4.2.2(b)	N/A	assurance that backup copies are complete and accurate, including configuration data and data stored in cloud computing service environment;	Functional	intersects with	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	5	
4.2.2(c)	N/A	storing backup copies (online or offline) in a safe location or locations, which are not in the same network as the system, and are at sufficient distance to escape any damage from a disaster at the main site;	Functional	intersects with	Alternate Storage & Processing Sites	BCD-04.2	Mechanisms exist to test contingency plans at alternate storage & processing sites to both familiarize contingency personnel with the facility and evaluate the capabilities of the alternate processing site to support contingency operations.	5	
4.2.2(c)	N/A	storing backup copies (online or offline) in a safe location or locations, which are not in the same network as the system, and are at sufficient distance to escape any damage from a disaster at the main site;	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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
4.2.2(d)	N/A	appropriate physical and logical access controls to backup copies, in accordance with the asset classification level;	Functional	intersects with	Backup Access	BCD-11.9	Mechanisms exist to restrict access to backups to privileged users with assigned roles for data backup and recovery operations.	8	
4.2.2(e)	N/A	restoring data from backup copies;	Functional	intersects with	Information System Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of systems to a known state after a disruption, compromise or failure.	5	
4.2.2(e)	N/A	restoring data from backup copies;	Functional	intersects with	Backup & Restoration Hardware Protection	BCD-13	Mechanisms exist to protect backup and restoration hardware and software.	5	
4.2.2(f)	N/A	retention periods based on business and regulatory requirements.	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 satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
4.2.2(f)	N/A	retention periods based on business and regulatory requirements.	Functional	subset of	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	10	
4.2.3	N/A	The relevant entities shall perform regular integrity checks on the backup copies.	Functional	intersects with	Backup & Restoration Hardware Protection	BCD-13	Mechanisms exist to protect backup and restoration hardware and software.	5	
4.2.3	N/A	The relevant entities shall perform regular integrity checks on the backup copies.	Functional	intersects with	Restoration Integrity Verification	BCD-13.1	Mechanisms exist to verify the integrity of backups and other restoration assets prior to using them for restoration.	8	
4.2.4	N/A	Based on the results of the risk assessment carried out pursuant to point 2.1 and the business continuity plan, the relevant entities shall ensure sufficient availability of resources by at least partial redundancy of the following:	Functional	subset of	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	10	
4.2.4(a)	N/A	network and information systems;	Functional	intersects with	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover system, which is not collocated with the primary system, application and/or service, which can be activated with little-to-no loss of information or disruption to operations.	5	
4.2.4(b)	N/A	assets, including facilities, equipment and supplies;	Functional	intersects with	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover system, which is not collocated with the primary system, application and/or service, which can be activated with little-to-no loss of information or disruption to operations.	5	
4.2.4(c)	N/A	personnel with the necessary responsibility, authority and competence;	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	10	
4.2.4(c)	N/A	personnel with the necessary responsibility, authority and competence;	Functional	intersects with	Establish Redundancy for Vital Cybersecurity & Data Privacy Staff	HRS-13.3	Mechanisms exist to establish redundancy for vital cybersecurity & data privacy staff.	8	
4.2.4(c)	N/A	personnel with the necessary responsibility, authority and competence;	Functional	intersects with	Manage Organizational Knowledge	PRM-08	Mechanisms exist to manage the organizational knowledge of the cybersecurity & data privacy staff.	5	
4.2.4(d)	N/A	appropriate communication channels.	Functional	intersects with	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover system, which is not collocated with the primary system, application and/or service, which can be activated with little-to-no loss of information or disruption to operations.	5	
4.2.5	N/A	Where appropriate, the relevant entities shall ensure that monitoring and adjustment of resources, including facilities, systems and personnel, is duly informed by backup and redundancy requirements.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
4.2.6	N/A	The relevant entities shall carry out regular testing of the recovery of backup copies and redundancies to ensure that, in recovery conditions, they can be relied upon and cover the copies, processes and knowledge to perform an effective recovery. The relevant entities shall document the results of the tests and, where needed, take corrective action.	Functional	subset of	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.	10	
4.3	Crisis management	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
4.3.1	N/A	The relevant entities shall put in place a process for crisis management.	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	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 (optional)	Notes (optional)
4.3.1	N/A	The relevant entities shall put in place a process for crisis management.	Functional	intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	8	
4.3.2	N/A	The relevant entities shall ensure that the crisis management process addresses at least the following elements:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
4.3.2(a)	N/A	roles and responsibilities for personnel and, where appropriate, suppliers and service providers, specifying the allocation of roles in crisis situations, including specific steps to follow;	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
4.3.2(a)	N/A	roles and responsibilities for personnel and, where appropriate, suppliers and service providers, specifying the allocation of roles in crisis situations, including specific steps to follow;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
4.3.2(a)	N/A	roles and responsibilities for personnel and, where appropriate, suppliers and service providers, specifying the allocation of roles in crisis situations, including specific steps to follow;	Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
4.3.2(b)	N/A	appropriate communication means between the relevant entities and relevant competent authorities;	Functional	intersects with	Alternate Communications Channels	BCD-10.4	Mechanisms exist to maintain command and control capabilities via alternate communications channels and designating alternative decision makers if primary decision makers are unavailable.	5	
4.3.2(c)	N/A	application of appropriate measures to ensure the maintenance of network and information system security in crisis situations. For the purpose of point (b), the flow of information between the relevant entities and relevant competent authorities shall include both obligatory communications, such as incident reports and related timelines, and non-obligatory communications.	Functional	subset of	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	10	
4.3.3	N/A	The relevant entities shall implement a process for managing and making use of information received from the CSIRTs or, where applicable, the competent authorities, concerning incidents, vulnerabilities, threats or possible mitigation measures.	Functional	subset of	Coordinate with Related Plans	BCD-01.1	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	10	
4.3.3	N/A	The relevant entities shall implement a process for managing and making use of information received from the CSIRTs or, where applicable, the competent authorities, concerning incidents, vulnerabilities, threats or possible mitigation measures.	Functional	intersects with	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
4.3.4	N/A	The relevant entities shall test, review and, where appropriate, update the crisis management plan on a regular basis or following significant incidents or significant changes to operations or risks.	Functional	subset of	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.	10	
5	SUPPLY CHAIN SECURITY (ARTICLE 21(2), POINT (D), OF DIRECTIVE (EU) 2022/2555)	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
5.1	Supply chain security policy	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
5.1.1	N/A	For the purpose of Article 21(2), point (d) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a supply chain security policy which governs the relations with their direct suppliers and service providers in order to mitigate the identified risks to the security of network and information systems. In the supply chain security policy, the relevant entities shall identify their role in the supply chain and communicate it to their direct suppliers and service providers.	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
5.1.1	N/A	For the purpose of Article 21(2), point (d) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a supply chain security policy which governs the relations with their direct suppliers and service providers in order to mitigate the identified risks to the security of network and information systems. In the supply chain security policy, the relevant entities shall identify their role in the supply chain and communicate it to their direct suppliers and service providers.	Functional	subset of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
5.1.2	N/A	As part of the supply chain security policy referred to in point 5.1.1, the relevant entities shall lay down criteria to select and contract suppliers and service providers. Those criteria shall include the following:	Functional	subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	10	
5.1.2(a)	N/A	the cybersecurity practices of the suppliers and service providers, including their secure development procedures;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
5.1.2(b)	N/A	the ability of the suppliers and service providers to meet cybersecurity specifications set by the relevant entities;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
5.1.2(c)	N/A	the overall quality and resilience of ICT products and ICT services and the cybersecurity risk-management measures embedded in them, including the risks and classification level of the ICT products and ICT services;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
5.1.2(d)	N/A	the ability of the relevant entities to diversify sources of supply and limit vendor lock-in, where applicable.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
5.1.3	N/A	When establishing their supply chain security policy, relevant entities shall take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1) of Directive (EU) 2022/2555, where applicable.	Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	5	
5.1.4	N/A	Based on the supply chain security policy and taking into account the results of the risk assessment carried out in accordance with point 2.1. of this Annex, the relevant entities shall ensure that their contracts with the suppliers and service providers specify, where appropriate through service level agreements, the following, where appropriate:	Functional	subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	10	
5.1.4(a)	N/A	cybersecurity requirements for the suppliers or service providers, including requirements as regards the security in acquisition of ICT services or ICT products set out in point 6.1.;	Functional	subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	10	
5.1.4(b)	N/A	requirements regarding awareness, skills and training, and where appropriate certifications, required from the suppliers' or service providers' employees;	Functional	subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	10	
5.1.4(c)	N/A	requirements regarding the verification of the background of the suppliers' and service providers' employees;	Functional	intersects with	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	8	
5.1.4(c)	N/A	requirements regarding the verification of the background of the suppliers' and service providers' employees;	Functional	subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	10	
5.1.4(d)	N/A	an obligation on suppliers and service providers to notify, without undue delay, the relevant entities of incidents that present a risk to the security of the network and information systems of those entities;	Functional	subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	10	
5.1.4(e)	N/A	the right to audit or right to receive audit reports;	Functional	subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	10	
5.1.4(f)	N/A	an obligation on suppliers and service providers to handle vulnerabilities that present a risk to the security of the network and information systems of the relevant entities;	Functional	subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	10	
5.1.4(g)	N/A	requirements regarding subcontracting and, where the relevant entities allow subcontracting, cybersecurity requirements for subcontractors in accordance with the cybersecurity requirements referred to in point (a);	Functional	subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	10	
5.1.4(g)	N/A	requirements regarding subcontracting and, where the relevant entities allow subcontracting, cybersecurity requirements for subcontractors in accordance with the cybersecurity requirements referred to in point (a);	Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	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 (optional)	Notes (optional)
5.1.4(h)	N/A	obligations on the suppliers and service providers at the termination of the contract, such as retrieval and disposal of the information obtained by the suppliers and service providers in the exercise of their tasks.	Functional	subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	10	
5.1.5	N/A	The relevant entities shall take into account the elements referred to in point 5.1.2 and 5.1.3. as part of the selection process of new suppliers and service providers, as well as part of the procurement process referred to in point 6.1.	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	8	
5.1.5	N/A	The relevant entities shall take into account the elements referred to in point 5.1.2 and 5.1.3. as part of the selection process of new suppliers and service providers, as well as part of the procurement process referred to in point 6.1.	Functional	subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	10	
5.1.6	N/A	The relevant entities shall review the supply chain security policy, and monitor, evaluate and, where necessary, act upon changes in the cybersecurity practices of suppliers and service providers, at planned intervals and when significant changes to operations or risks or significant incidents related to the provision of ICT services or having impact on the security of the ICT products from suppliers and service providers occur.	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
5.1.6	N/A	The relevant entities shall review the supply chain security policy, and monitor, evaluate and, where necessary, act upon changes in the cybersecurity practices of suppliers and service providers, at planned intervals and when significant changes to operations or risks or significant incidents related to the provision of ICT services or having impact on the security of the ICT products from suppliers and service providers occur.	Functional	intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
5.1.6	N/A	The relevant entities shall review the supply chain security policy, and monitor, evaluate and, where necessary, act upon changes in the cybersecurity practices of suppliers and service providers, at planned intervals and when significant changes to operations or risks or significant incidents related to the provision of ICT services or having impact on the security of the ICT products from suppliers and service providers occur.	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
5.1.6	N/A	The relevant entities shall review the supply chain security policy, and monitor, evaluate and, where necessary, act upon changes in the cybersecurity practices of suppliers and service providers, at planned intervals and when significant changes to operations or risks or significant incidents related to the provision of ICT services or having impact on the security of the ICT products from suppliers and service providers occur.	Functional	subset of	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with the services and product supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	10	
5.1.7	N/A	For the purpose of point 5.1.6., the relevant entities shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
5.1.7(a)	N/A	regularly monitor reports on the implementation of the service level agreements, where applicable;	Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
5.1.7(b)	N/A	review incidents related to ICT products and ICT services from suppliers and service providers;	Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
5.1.7(c)	N/A	assess the need for unscheduled reviews and document the findings in a comprehensible manner;	Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
5.1.7(d)	N/A	analyse the risks presented by changes related to ICT products and ICT services from suppliers and service providers and, where appropriate, take mitigating measures in a timely manner.	Functional	subset of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
5.1.7(d)	N/A	analyse the risks presented by changes related to ICT products and ICT services from suppliers and service providers and, where appropriate, take mitigating measures in a timely manner.	Functional	intersects with	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business information, systems and processes that are in scope by the third-party.	8	
5.2	Directory of suppliers and service providers	The relevant entities shall maintain and keep up to date a registry of their direct suppliers and service providers, including:	Functional	subset of	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.	10	
5.2(a)	N/A	contact points for each direct supplier and service provider;	Functional	subset of	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.	10	
5.2(b)	N/A	a list of ICT products, ICT services, and ICT processes provided by the direct supplier or service provider to the relevant entities.	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8	
6	SECURITY IN NETWORK AND INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE (ARTICLE 21(2), POINT (E), OF DIRECTIVE (EU) 2022/2555)	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.1	Security in acquisition of ICT services or ICT products	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.1.1	N/A	For the purpose of Article 21(2), point (e) of Directive (EU) 2022/2555, the relevant entities shall set and implement processes to manage risks stemming from the acquisition of ICT services or ICT products for components that are critical for the relevant entities' security of network and information systems, based on the risk assessment carried out pursuant to point 2.1, from suppliers or service providers throughout their life cycle.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
6.1.1	N/A	For the purpose of Article 21(2), point (e) of Directive (EU) 2022/2555, the relevant entities shall set and implement processes to manage risks stemming from the acquisition of ICT services or ICT products for components that are critical for the relevant entities' security of network and information systems, based on the risk assessment carried out pursuant to point 2.1, from suppliers or service providers throughout their life cycle.	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 systems and data.	5	
6.1.2	N/A	For the purpose of point 6.1.1., the processes referred to in point 6.1.1. shall include:	Functional	subset of	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	10	
6.1.2(a)	N/A	security requirements to apply to the ICT services or ICT products to be acquired;	Functional	subset of	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	10	
6.1.2(b)	N/A	requirements regarding security updates throughout the entire lifetime of the ICT services or ICT products, or replacement after the end of the support period;	Functional	subset of	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	10	
6.1.2(c)	N/A	information describing the hardware and software components used in the ICT services or ICT products;	Functional	intersects with	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	10	
6.1.2(d)	N/A	information describing the implemented cybersecurity functions of the ICT services or ICT products and the configuration required for their secure operation;	Functional	subset of	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	10	
6.1.2(e)	N/A	assurance that the ICT services or ICT products comply with the security requirements according to point (a);	Functional	subset of	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	10	
6.1.2(f)	N/A	methods for validating that the delivered ICT services or ICT products are compliant to the stated security requirements, as well as documentation of the results of the validation.	Functional	subset of	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	10	
6.1.3	N/A	The relevant entities shall review and, where appropriate, update the processes at planned intervals and when significant incidents occur.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
6.1.3	N/A	The relevant entities shall review and, where appropriate, update the processes at planned intervals and when significant incidents occur.	Functional	intersects with	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	8	
6.2	Secure development life cycle	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.2.1	N/A	Before developing a network and information system, including software, the relevant entities shall lay down rules for the secure development of network and information systems and apply them when developing network and information systems in-house, or when outsourcing the development of network and information systems. The rules shall cover all development phases, including specification, design, development, implementation and testing.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	8	
6.2.1	N/A	Before developing a network and information system, including software, the relevant entities shall lay down rules for the secure development of network and information systems and apply them when developing network and information systems in-house, or when outsourcing the development of network and information systems. The rules shall cover all development phases, including specification, design, development, implementation and testing.	Functional	subset of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
6.2.1	N/A	Before developing a network and information system, including software, the relevant entities shall lay down rules for the secure development of network and information systems and apply them when developing network and information systems in-house, or when outsourcing the development of network and information systems. The rules shall cover all development phases, including specification, design, development, implementation and testing.	Functional	intersects with	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	
6.2.2	N/A	For the purpose of point 6.2.1., the relevant entities shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.2.2(a)	N/A	carry out an analysis of security requirements at the specification and design phases of any development or acquisition project undertaken by the relevant entities or on behalf of those entities;	Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
6.2.2(a)	N/A	carry out an analysis of security requirements at the specification and design phases of any development or acquisition project undertaken by the relevant entities or on behalf of those entities;	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
6.2.2(b)	N/A	apply principles for engineering secure systems and secure coding principles to any information system development activities such as promoting cybersecurity-by-design, zero-trust architectures;	Functional	subset of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
6.2.2(c)	N/A	lay down security requirements regarding development environments;	Functional	subset of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
6.2.2(c)	N/A	lay down security requirements regarding development environments;	Functional	intersects with	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	
6.2.2(c)	N/A	lay down security requirements regarding development environments;	Functional	intersects with	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5	
6.2.2(d)	N/A	establish and implement security testing processes in the development life cycle;	Functional	intersects with	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	8	
6.2.2(e)	N/A	appropriately select, protect and manage security test data;	Functional	intersects with	Test Data Integrity	TDA-10.1	Mechanisms exist to ensure the integrity of test data through existing cybersecurity & data privacy controls.	5	
6.2.2(f)	N/A	sanitise and anonymise testing data according to the risk assessment carried out pursuant to point 2.1.	Functional	intersects with	Limit Sensitive / Regulated Data In Testing, Training & Research	DCH-18.2	Mechanisms exist to minimize the use of sensitive/regulated data for research, testing, or training, in accordance with authorized, legitimate business practices.	5	
6.2.2(f)	N/A	sanitise and anonymise testing data according to the risk assessment carried out pursuant to point 2.1.	Functional	subset of	Use of Live Data	TDA-10	Mechanisms exist to approve, document and control the use of live data in development and test environments.	10	
6.2.3	N/A	For outsourced development of network and information systems, the relevant entities shall also apply the policies and procedures referred to in points 5 and 6.1.	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
6.2.3	N/A	For outsourced development of network and information systems, the relevant entities shall also apply the policies and procedures referred to in points 5 and 6.1.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	8	
6.2.3	N/A	For outsourced development of network and information systems, the relevant entities shall also apply the policies and procedures referred to in points 5 and 6.1.	Functional	subset of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	10	
6.2.4	N/A	The relevant entities shall review and, where necessary, update their secure development rules at planned intervals.	Functional	subset of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
6.3	Configuration management	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.3.1	N/A	The relevant entities shall take the appropriate measures to establish, document, implement, and monitor configurations, including security configurations of hardware, software, services and networks.	Functional	subset of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
6.3.2	N/A	For the purpose of point 6.3.1., the relevant entities shall:	Functional	subset of	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
6.3.2(a)	N/A	lay down and ensure security in configurations for their hardware, software, services and networks;	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	8	
6.3.2(b)	N/A	lay down and implement processes and tools to enforce the laid down secure configurations for hardware, software, services and networks, for newly installed systems as well as for systems in operation over their lifetime.	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	8	
6.3.3	N/A	The relevant entities shall review and, where appropriate, update configurations at planned intervals or when significant incidents or significant changes to operations or risks occur.	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
6.3.3	N/A	The relevant entities shall review and, where appropriate, update configurations at planned intervals or when significant incidents or significant changes to operations or risks occur.	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	
6.4	Change management, repairs and maintenance	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.4.1	N/A	The relevant entities shall apply change management procedures to control changes of network and information systems. Where applicable, the procedures shall be consistent with the relevant entities' general policies concerning change management.	Functional	subset of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
6.4.1	N/A	The relevant entities shall apply change management procedures to control changes of network and information systems. Where applicable, the procedures shall be consistent with the relevant entities' general policies concerning change management.	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
6.4.2	N/A	The procedures referred to in point 6.4.1. shall be applied for releases, modifications and emergency changes of any software and hardware in operation and changes to the configuration. The procedures shall ensure that those changes are documented and, based on the risk assessment carried out pursuant to point 2.1, tested and assessed in view of the potential impact before being implemented.	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
6.4.2	N/A	The procedures referred to in point 6.4.1. shall be applied for releases, modifications and emergency changes of any software and hardware in operation and changes to the configuration. The procedures shall ensure that those changes are documented and, based on the risk assessment carried out pursuant to point 2.1, tested and assessed in view of the potential impact before being implemented.	Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
6.4.3	N/A	In the event that the regular change management procedures could not be followed due to an emergency, the relevant entities shall document the result of the change, and the explanation for why the procedures could not be followed.	Functional	intersects with	Emergency Changes	CHG-07	Mechanisms exist to govern change management procedures for "emergency" changes.	10	
6.4.3	N/A	In the event that the regular change management procedures could not be followed due to an emergency, the relevant entities shall document the result of the change, and the explanation for why the procedures could not be followed.	Functional	intersects with	Documenting Emergency Changes	CHG-07.1	Mechanisms exist to document the results of "emergency" changes, including an explanation for why standard change management procedures could not be followed.	10	
6.4.4	N/A	The relevant entities shall review and, where appropriate, update the procedures at planned intervals and when significant incidents or significant changes to operations or risks.	Functional	subset of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
6.5	Security testing	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.5.1	N/A	The relevant entities shall establish, implement and apply a policy and procedures for security testing.	Functional	subset of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	10	
6.5.1	N/A	The relevant entities shall establish, implement and apply a policy and procedures for security testing.	Functional	intersects with	Cybersecurity & Data Privacy Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity & data privacy personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	5	
6.5.2	N/A	The relevant entities shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.5.2(a)	N/A	establish, based on the risk assessment carried out pursuant to point 2.1, the need, scope, frequency and type of security tests;	Functional	subset of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	10	
6.5.2(a)	N/A	establish, based on the risk assessment carried out pursuant to point 2.1, the need, scope, frequency and type of security tests;	Functional	intersects with	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity & data privacy controls in systems, applications and services 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.	8	
6.5.2(b)	N/A	carry out security tests according to a documented test methodology, covering the components identified as relevant for secure operation in a risk analysis;	Functional	intersects with	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity & data privacy controls in systems, applications and services 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.	8	
6.5.2(c)	N/A	document the type, scope, time and results of the tests, including assessment of criticality and mitigating actions for each finding;	Functional	intersects with	Assessment Boundaries	IAO-01.1	Mechanisms exist to establish the scope of assessments by defining the assessment boundary, according to people, processes and technology that directly or indirectly impact the confidentiality, integrity, availability and safety of the data and systems under review.	5	
6.5.2(c)	N/A	document the type, scope, time and results of the tests, including assessment of criticality and mitigating actions for each finding;	Functional	subset of	Security Assessment Report (SAR)	IAO-02.4	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	10	
6.5.2(d)	N/A	apply mitigating actions in case of critical findings.	Functional	subset of	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	10	
6.5.3	N/A	The relevant entities shall review and, where appropriate, update their security testing policies at planned intervals.	Functional	subset of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	10	
6.6	Security patch management	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.6.1	N/A	The relevant entities shall specify and apply procedures, coherent with the change management procedures referred to in point 6.4.1. as well as with vulnerability management, risk management and other relevant management procedures, for ensuring that:	Functional	intersects with	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	8	
6.6.1	N/A	The relevant entities shall specify and apply procedures, coherent with the change management procedures referred to in point 6.4.1. as well as with vulnerability management, risk management and other relevant management procedures, for ensuring that:	Functional	intersects with	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	8	
6.6.1(a)	N/A	security patches are applied within a reasonable time after they become available;	Functional	intersects with	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	8	
6.6.1(b)	N/A	security patches are tested before being applied in production systems;	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	
6.6.1(c)	N/A	security patches come from trusted sources and are checked for integrity;	Functional	intersects with	Software / Firmware Integrity Verification	TDA-14.1	Mechanisms exist to require developer of systems, system components or services to enable integrity verification of software and firmware components.	3	
6.6.1(c)	N/A	security patches come from trusted sources and are checked for integrity;	Functional	subset of	Software Patch Integrity	VPM-05.8	Mechanisms exist to ensure software and/or firmware patches are: (1) Obtained from trusted sources; and (2) Checked for integrity.	10	
6.6.1(d)	N/A	additional measures are implemented and residual risks are accepted in cases where a patch is not available or not applied pursuant to point 6.6.2.	Functional	subset of	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	10	
6.6.2	N/A	By way of derogation from point 6.6.1.(a), the relevant entities may choose not to apply security patches when the disadvantages of applying the security patches outweigh the cybersecurity benefits. The relevant entities shall duly document and substantiate the reasons for any such decision.	Functional	subset of	Deferred Patching Decisions	VPM-04.3	Mechanisms exist to facilitate the deferral of software and/or firmware patches when the disadvantages of applying the patch outweighs the benefits.	10	
6.7	Network security	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.7.1	N/A	The relevant entities shall take the appropriate measures to protect their network and information systems from cyber threats.	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
6.7.1	N/A	The relevant entities shall take the appropriate measures to protect their network and information systems from cyber threats.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	8	
6.7.2	N/A	For the purpose of point 6.7.1., the relevant entities shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.7.2(a)	N/A	document the architecture of the network in a comprehensible and up to date manner;	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	
6.7.2(b)	N/A	determine and apply controls to protect the relevant entities' internal network domains from unauthorised access;	Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
6.7.2(c)	N/A	configure controls to prevent accesses and network communication not required for the operation of the relevant entities;	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	
6.7.2(d)	N/A	determine and apply controls for remote access to network and information systems, including access by service providers;	Functional	intersects with	Remote Access	NET-14	Mechanisms exist to define, control and review organization-approved, secure remote access methods.	8	
6.7.2(e)	N/A	not use systems used for administration of the security policy implementation for other purposes;	Functional	intersects with	Dedicated Administrative Machines	IAC-20.4	Mechanisms exist to restrict executing administrative tasks or tasks requiring elevated access to a dedicated machine.	8	
6.7.2(f)	N/A	explicitly forbid or deactivate unneeded connections and services;	Functional	subset of	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	
6.7.2(f)	N/A	explicitly forbid or deactivate unneeded connections and services;	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	
6.7.2(g)	N/A	where appropriate, exclusively allow access to the relevant entities' network and information systems by devices authorised by those entities;	Functional	subset of	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	
6.7.2(g)	N/A	where appropriate, exclusively allow access to the relevant entities' network and information systems by devices authorised by those entities;	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	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
6.7.2(h)	N/A	allow connections of service providers only after an authorisation request and for a set time period, such as the duration of a maintenance operation;	Functional	subset of	Remote Maintenance	MNT-05	Mechanisms exist to authorize, monitor and control remote, non-local maintenance and diagnostic activities.	10	
6.7.2(i)	N/A	establish communication between distinct systems only through trusted channels that are isolated using logical, cryptographic or physical separation from other communication channels and provide assured identification of their end points and protection of the channel data from modification or disclosure;	Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
6.7.2(j)	N/A	adopt an implementation plan for the full transition towards latest generation network layer communication protocols in a secure, appropriate and gradual way and establish measures to accelerate such transition;	Functional	subset of	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.	10	
6.7.2(k)	N/A	adopt an implementation plan for the deployment of internationally agreed and interoperable modern e-mail communications standards to secure e-mail communications to mitigate vulnerabilities linked to e-mail-related threats and establish measures to accelerate such deployment;	Functional	subset of	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.	10	
6.7.2(l)	N/A	apply best practices for the security of the DNS, and for Internet routing security and routing hygiene of traffic originating from and destined to the network.	Functional	subset of	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.	10	
6.7.2(l)	N/A	apply best practices for the security of the DNS, and for Internet routing security and routing hygiene of traffic originating from and destined to the network.	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.	3	
6.7.3	N/A	The relevant entities shall review and, where appropriate, update these measures at planned intervals and when significant incidents or significant changes to operations or risks occur.	Functional	intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity & data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
6.7.3	N/A	The relevant entities shall review and, where appropriate, update these measures at planned intervals and when significant incidents or significant changes to operations or risks occur.	Functional	subset of	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.	10	
6.8	Network segmentation	Network segmentation	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.8.1	N/A	The relevant entities shall segment systems into networks or zones in accordance with the results of the risk assessment referred to in point 2.1. They shall segment their systems and networks from third parties' systems and networks.	Functional	subset of	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	10	
6.8.2	N/A	For that purpose, the relevant entities shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.8.2(a)	N/A	consider the functional, logical and physical relationship, including location, between trustworthy systems and services;	Functional	subset of	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	10	
6.8.2(b)	N/A	grant access to a network or zone based on an assessment of its security requirements;	Functional	subset of	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	10	
6.8.2(c)	N/A	keep systems that are critical to the relevant entities operation or to safety in secured zones;	Functional	subset of	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	10	
6.8.2(d)	N/A	deploy a demilitarised zone within their communication networks to ensure secure communication originating from or destined to their networks;	Functional	subset of	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	10	
6.8.2(d)	N/A	deploy a demilitarised zone within their communication networks to ensure secure communication originating from or destined to their networks;	Functional	intersects with	DMZ Networks	NET-08.1	Mechanisms exist to monitor De-Militarized Zone (DMZ) network segments to separate untrusted networks from trusted networks.	8	
6.8.2(e)	N/A	restrict access and communications between and within zones to those necessary for the operation of the relevant entities or for safety;	Functional	subset of	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	10	
6.8.2(e)	N/A	restrict access and communications between and within zones to those necessary for the operation of the relevant entities or for safety;	Functional	subset of	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	10	
6.8.2(f)	N/A	separate the dedicated network for administration of network and information systems from the relevant entities' operational network;	Functional	subset of	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	10	
6.8.2(f)	N/A	separate the dedicated network for administration of network and information systems from the relevant entities' operational network;	Functional	subset of	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	10	
6.8.2(g)	N/A	segregate network administration channels from other network traffic;	Functional	subset of	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	10	
6.8.2(h)	N/A	separate the production systems for the relevant entities' services from systems used in development and testing, including backups.	Functional	subset of	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	10	
6.8.2(h)	N/A	separate the production systems for the relevant entities' services from systems used in development and testing, including backups.	Functional	intersects with	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	8	
6.8.3	N/A	The relevant entities shall review and, where appropriate, update network segmentation at planned intervals and when significant incidents or significant changes to operations or risks.	Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
6.9	Protection against malicious and unauthorised software	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.9.1	N/A	The relevant entities shall protect their network and information systems against malicious and unauthorised software.	Functional	intersects with	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	8	
6.9.1	N/A	The relevant entities shall protect their network and information systems against malicious and unauthorised software.	Functional	intersects with	Endpoint Security	END-01	Mechanisms exist to facilitate the implementation of endpoint security controls.	8	
6.9.1	N/A	The relevant entities shall protect their network and information systems against malicious and unauthorised software.	Functional	intersects with	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	8	
6.9.2	N/A	For that purpose, the relevant entities shall in particular implement measures that detect or prevent the use of malicious or unauthorised software. The relevant entities shall, where appropriate, ensure that their network and information systems are equipped with detection and response software, which is updated regularly in accordance with the risk assessment carried out pursuant to point 2.1 and the contractual agreements with the providers.	Functional	subset of	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	10	
6.9.2	N/A	For that purpose, the relevant entities shall in particular implement measures that detect or prevent the use of malicious or unauthorised software. The relevant entities shall, where appropriate, ensure that their network and information systems are equipped with detection and response software, which is updated regularly in accordance with the risk assessment carried out pursuant to point 2.1 and the contractual agreements with the providers.	Functional	intersects with	Automatic Antimalware Signature Updates	END-04.1	Mechanisms exist to automatically update antimalware technologies, including signature definitions.	8	
6.10	Vulnerability handling and disclosure	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.10.1	N/A	The relevant entities shall obtain information about technical vulnerabilities in their network and information systems, evaluate their exposure to such vulnerabilities, and take appropriate measures to manage the vulnerabilities.	Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
6.10.1	N/A	The relevant entities shall obtain information about technical vulnerabilities in their network and information systems, evaluate their exposure to such vulnerabilities, and take appropriate measures to manage the vulnerabilities.	Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	8	
6.10.2	N/A	For the purpose of point 6.10.1., the relevant entities shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
6.10.2(a)	N/A	monitor information about vulnerabilities through appropriate channels, such as announcements of CSIRTs, competent authorities or information provided by suppliers or service providers;	Functional	intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity & data privacy incidents to internal stakeholders all the way through the resolution of the incident.	8	
6.10.2(a)	N/A	monitor information about vulnerabilities through appropriate channels, such as announcements of CSIRTs, competent authorities or information provided by suppliers or service providers;	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.	8	
6.10.2(a)	N/A	monitor information about vulnerabilities through appropriate channels, such as announcements of CSIRTs, competent authorities or information provided by suppliers or service providers;	Functional	intersects with	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	8	
6.10.2(b)	N/A	perform, where appropriate, vulnerability scans, and record evidence of the results of the scans, at planned intervals;	Functional	equal	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	10	
6.10.2(c)	N/A	address, without undue delay, vulnerabilities identified by the relevant entities as critical to their operations;	Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	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 (optional)	Notes (optional)
6.10.2(d)	N/A	ensure that their vulnerability handling is compatible with their change management, security patch management, risk management and incident management procedures;	Functional	intersects with	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	8	
6.10.2(d)	N/A	ensure that their vulnerability handling is compatible with their change management, security patch management, risk management and incident management procedures;	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.	8	
6.10.2(d)	N/A	ensure that their vulnerability handling is compatible with their change management, security patch management, risk management and incident management procedures;	Functional	intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	
6.10.2(d)	N/A	ensure that their vulnerability handling is compatible with their change management, security patch management, risk management and incident management procedures;	Functional	intersects with	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	8	
6.10.2(e)	N/A	lay down a procedure for disclosing vulnerabilities in accordance with the applicable national coordinated vulnerability disclosure policy.	Functional	subset of	Disclosure of Vulnerabilities	TDA-02.11	Mechanisms exist to disclose information about vulnerabilities to relevant stakeholders, including: (1) A description of the vulnerability(ies); (2) Affected product(s) and/or service(s); (3) Potential impact of the vulnerability(ies); (4) Severity of the vulnerability(ies); and (5) Guidance to remediate the vulnerability(ies).	10	
6.10.3	N/A	When justified by the potential impact of the vulnerability, the relevant entities shall create and implement a plan to mitigate the vulnerability. In other cases, the relevant entities shall document and substantiate the reason why the vulnerability does not require remediation.	Functional	subset of	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	10	
6.10.4	N/A	The relevant entities shall review and, where appropriate, update at planned intervals the channels they use for monitoring vulnerability information.	Functional	intersects with	Automated Software & Firmware Updates	VPM-05.4	Automated mechanisms exist to install the latest stable versions of security-relevant software and firmware updates.	8	
6.10.4	N/A	The relevant entities shall review and, where appropriate, update at planned intervals the channels they use for monitoring vulnerability information.	Functional	intersects with	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	8	
7	POLICIES AND PROCEDURES TO ASSESS THE EFFECTIVENESS OF CYBERSECURITY RISK-MANAGEMENT MEASURES (ARTICLE 21(2), POINT (F), OF DIRECTIVE (EU) 2022/2555)	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
7.1	N/A	For the purpose of Article 21(2), point (f) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a policy and procedures to assess whether the cybersecurity risk-management measures taken by the relevant entity are effectively implemented and maintained.	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
7.1	N/A	For the purpose of Article 21(2), point (f) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a policy and procedures to assess whether the cybersecurity risk-management measures taken by the relevant entity are effectively implemented and maintained.	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.	8	
7.1	N/A	For the purpose of Article 21(2), point (f) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a policy and procedures to assess whether the cybersecurity risk-management measures taken by the relevant entity are effectively implemented and maintained.	Functional	intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	8	
7.2	N/A	The policy and procedures referred to in point 7.1. shall take into account results of the risk assessment pursuant to point 2.1. and past significant incidents. The relevant entities shall determine:	Functional	subset of	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	10	
7.2(a)	N/A	what cybersecurity risk-management measures are to be monitored and measured, including processes and controls;	Functional	subset of	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	10	
7.2(b)	N/A	the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;	Functional	subset of	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	10	
7.2(c)	N/A	when the monitoring and measuring is to be performed;	Functional	subset of	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	10	
7.2(d)	N/A	who is responsible for monitoring and measuring the effectiveness of the cybersecurity risk-management measures;	Functional	subset of	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	10	
7.2(e)	N/A	when the results from monitoring and measurement are to be analysed and evaluated;	Functional	subset of	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	10	
7.2(f)	N/A	who has to analyse and evaluate these results.	Functional	subset of	Risk Assessment Methodology	RSK-04.2	Mechanisms exist to implement a risk assessment methodology to ensure coverage for organizational components relevant for secure, compliant and resilient operations.	10	
7.3	N/A	The relevant entities shall review and, where appropriate, update the policy and procedures at planned intervals and when significant incidents or significant changes to operations or risks.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
8	BASIC CYBER HYGIENE PRACTICES AND SECURITY TRAINING (ARTICLE 21(2), POINT (G), OF DIRECTIVE (EU) 2022/2555)	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
8.1	Awareness raising and basic cyber hygiene practices	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
8.1.1	N/A	For the purpose of Article 21(2), point (g) of Directive (EU) 2022/2555, the relevant entities shall ensure that their employees, including members of management bodies, as well as direct suppliers and service providers are aware of risks, are informed of the importance of cybersecurity and apply cyber hygiene practices.	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.	8	
8.1.1	N/A	For the purpose of Article 21(2), point (g) of Directive (EU) 2022/2555, the relevant entities shall ensure that their employees, including members of management bodies, as well as direct suppliers and service providers are aware of risks, are informed of the importance of cybersecurity and apply cyber hygiene practices.	Functional	intersects with	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	8	
8.1.1	N/A	For the purpose of Article 21(2), point (g) of Directive (EU) 2022/2555, the relevant entities shall ensure that their employees, including members of management bodies, as well as direct suppliers and service providers are aware of risks, are informed of the importance of cybersecurity and apply cyber hygiene practices.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	8	
8.1.1	N/A	For the purpose of Article 21(2), point (g) of Directive (EU) 2022/2555, the relevant entities shall ensure that their employees, including members of management bodies, as well as direct suppliers and service providers are aware of risks, are informed of the importance of cybersecurity and apply cyber hygiene practices.	Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	8	
8.1.2	N/A	For the purpose of point 8.1.1., the relevant entities shall offer to their employees, including members of management bodies, as well as to direct suppliers and service providers where appropriate in accordance with point 5.1.4., an awareness raising programme, which shall:	Functional	subset of	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	
8.1.2(a)	N/A	be scheduled over time, so that the activities are repeated and cover new employees;	Functional	subset of	Maintaining Workforce Development Relevancy	SAT-01.1	Mechanisms exist to periodically review security workforce development and awareness training to account for changes to: (1) Organizational policies, standards and procedures; (2) Assigned roles and responsibilities; (3) Relevant threats and risks; and (4) Technological developments.	10	
8.1.2(b)	N/A	be established in line with the network and information security policy, topic-specific policies and relevant procedures on network and information security;	Functional	intersects with	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity & data privacy awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
8.1.2(c)	N/A	cover relevant cyber threats, the cybersecurity risk-management measures in place, contact points and resources for additional information and advice on cybersecurity matters, as well as cyber hygiene practices for users.	Functional	intersects with	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity & data privacy awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	8	
8.1.3	N/A	The awareness raising programme shall, where appropriate, be tested in terms of effectiveness. The awareness raising programme shall be updated and offered at planned intervals taking into account changes in cyber hygiene practices, and the current threat landscape and risks posed to the relevant entities.	Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
8.2	Security training	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
8.2.1	N/A	The relevant entities shall identify employees, whose roles require security relevant skill sets and expertise, and ensure that they receive regular training on network and information system security.	Functional	subset of	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	10	
8.2.2	N/A	The relevant entities shall establish, implement and apply a training program in line with the network and information security policy, topic-specific policies and other relevant procedures on network and information security which lays down the training needs for certain roles and positions based on criteria.	Functional	subset of	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	10	
8.2.3	N/A	The training referred to in point 8.2.1. shall be relevant to the job function of the employee and its effectiveness shall be assessed. Training shall take into consideration security measures in place and cover the following:	Functional	subset of	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	10	
8.2.3(a)	N/A	instructions regarding the secure configuration and operation of the network and information systems, including mobile devices;	Functional	subset of	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	10	
8.2.3(b)	N/A	briefing on known cyber threats;	Functional	intersects with	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity & data privacy awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	8	
8.2.3(c)	N/A	training of the behaviour when security-relevant events occur.	Functional	subset of	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	10	
8.2.4	N/A	The relevant entities shall apply training to staff members who transfer to new positions or roles which require security relevant skill sets and expertise.	Functional	subset of	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	10	
8.2.5	N/A	The program shall be updated and run periodically taking into account applicable policies and rules, assigned roles, responsibilities, as well as known cyber threats and technological developments.	Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
9	CRYPTOGRAPHY (ARTICLE 21(2), POINT (H), OF DIRECTIVE (EU) 2022/2555)	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
9.1	N/A	For the purpose of Article 21(2), point (h) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a policy and procedures related to cryptography, with a view to ensuring adequate and effective use of cryptography to protect the confidentiality, authenticity and integrity of data in line with the relevant entities' asset classification and the results of the risk assessment carried out pursuant to point 2.1.	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	
9.1	N/A	For the purpose of Article 21(2), point (h) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a policy and procedures related to cryptography, with a view to ensuring adequate and effective use of cryptography to protect the confidentiality, authenticity and integrity of data in line with the relevant entities' asset classification and the results of the risk assessment carried out pursuant to point 2.1.	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
9.1	N/A	For the purpose of Article 21(2), point (h) of Directive (EU) 2022/2555, the relevant entities shall establish, implement and apply a policy and procedures related to cryptography, with a view to ensuring adequate and effective use of cryptography to protect the confidentiality, authenticity and integrity of data in line with the relevant entities' asset classification and the results of the risk assessment carried out pursuant to point 2.1.	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	
9.2	N/A	The policy and procedures referred to in point 9.1 shall establish:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
9.2(a)	N/A	in accordance with the relevant entities' classification of assets, the type, strength and quality of the cryptographic measures required to protect the relevant entities' assets, including data at rest and data in transit;	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	
9.2(b)	N/A	based on point (a), the protocols or families of protocols to be adopted, as well as cryptographic algorithms, cipher strength, cryptographic solutions and usage practices to be approved and required for use in the relevant entities, following, where appropriate, a cryptographic agility approach;	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	
9.2(c)	N/A	the relevant entities' approach to key management, including, where appropriate, methods for the following:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
9.2(c)(i)	N/A	generating different keys for cryptographic systems and applications;	Functional	intersects with	Control & Distribution of Cryptographic Keys	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	5	
9.2(c)(ii)	N/A	issuing and obtaining public key certificates;	Functional	intersects with	Control & Distribution of Cryptographic Keys	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	5	
9.2(c)(ii)	N/A	issuing and obtaining public key certificates;	Functional	intersects with	Certificate Authorities	CRY-11	Automated mechanisms exist to enable the use of organization-defined Certificate Authorities (CAs) to facilitate the establishment of protected sessions.	5	
9.2(c)(iii)	N/A	distributing keys to intended entities, including how to activate keys when received;	Functional	intersects with	Control & Distribution of Cryptographic Keys	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	5	
9.2(c)(iv)	N/A	storing keys, including how authorised users obtain access to keys;	Functional	intersects with	Control & Distribution of Cryptographic Keys	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	5	
9.2(c)(v)	N/A	changing or updating keys, including rules on when and how to change keys;	Functional	intersects with	Cryptographic Key Loss or Change	CRY-09.3	Mechanisms exist to ensure the availability of information in the event of the loss of cryptographic keys by individual users.	5	
9.2(c)(v)	N/A	changing or updating keys, including rules on when and how to change keys;	Functional	intersects with	Control & Distribution of Cryptographic Keys	CRY-09.4	Mechanisms exist to facilitate the secure distribution of symmetric and asymmetric cryptographic keys using industry recognized key management technology and processes.	5	
9.2(c)(vi)	N/A	dealing with compromised keys;	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	
9.2(c)(vii)	N/A	revoking keys including how to withdraw or deactivate keys;	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	
9.2(c)(viii)	N/A	recovering lost or corrupted keys;	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	
9.2(c)(ix)	N/A	backing up or archiving keys;	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	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
9.2(c)(x)	N/A	destroying keys;	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	
9.2(c)(xi)	N/A	logging and auditing of key management-related activities;	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	
9.2(c)(xii)	N/A	setting activation and deactivation dates for keys ensuring that the keys can only be used for the specified period of time according to the organization's rules on key management.	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	
9.3	N/A	The relevant entities shall review and, where appropriate, update their policy and procedures at planned intervals, taking into account the state of the art in cryptography.	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	
10	HUMAN RESOURCES SECURITY (ARTICLE 21(2), POINT (I), OF DIRECTIVE (EU) 2022/2555)	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
10.1	Human resources security	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
10.1.1	N/A	For the purpose of Article 21(2), point (i) of Directive (EU) 2022/2555, the relevant entities shall ensure that their employees and direct suppliers and service providers, wherever applicable, understand and commit to their security responsibilities, as appropriate for the offered services and the job and in line with the relevant entities' policy on the security of network and information systems.	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
10.1.1	N/A	For the purpose of Article 21(2), point (i) of Directive (EU) 2022/2555, the relevant entities shall ensure that their employees and direct suppliers and service providers, wherever applicable, understand and commit to their security responsibilities, as appropriate for the offered services and the job and in line with the relevant entities' policy on the security of network and information systems.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
10.1.2	N/A	The requirement referred to in point 10.1.1. shall include the following:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
10.1.2(a)	N/A	mechanisms to ensure that all employees, direct suppliers and service providers, wherever applicable, understand and follow the standard cyber hygiene practices that the relevant entities apply pursuant to point 8.1.;	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.	8	
10.1.2(a)	N/A	mechanisms to ensure that all employees, direct suppliers and service providers, wherever applicable, understand and follow the standard cyber hygiene practices that the relevant entities apply pursuant to point 8.1.;	Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
10.1.2(b)	N/A	mechanisms to ensure that all users with administrative or privileged access are aware of and act in accordance with their roles, responsibilities and authorities;	Functional	intersects with	Onboarding, Transferring & Offboarding Personnel	HRS-01.1	Mechanisms exist to proactively govern the following personnel management actions: (1) Onboarding new personnel (e.g., new hires); (2) Transferring personnel into new roles within the organization; and (3) Offboarding personnel (e.g., termination of employment).	5	
10.1.2(b)	N/A	mechanisms to ensure that all users with administrative or privileged access are aware of and act in accordance with their roles, responsibilities and authorities;	Functional	intersects with	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
10.1.2(b)	N/A	mechanisms to ensure that all users with administrative or privileged access are aware of and act in accordance with their roles, responsibilities and authorities;	Functional	intersects with	Users With Elevated Privileges	HRS-02.1	Mechanisms exist to ensure that every user accessing a system that processes, stores, or transmits sensitive information is cleared and regularly trained to handle the information in question.	5	
10.1.2(c)	N/A	mechanisms to ensure that members of management bodies understand and act in accordance with their role, responsibilities and authorities regarding network and information system security;	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	
10.1.2(d)	N/A	mechanisms for hiring personnel qualified for the respective roles, such as reference checks, vetting procedures, validation of certifications, or written tests.	Functional	subset of	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	
10.1.2(d)	N/A	mechanisms for hiring personnel qualified for the respective roles, such as reference checks, vetting procedures, validation of certifications, or written tests.	Functional	subset of	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	8	
10.1.3	N/A	The relevant entities shall review the assignment of personnel to specific roles as referred to in point 1.2., as well as their commitment of human resources in that regard, at planned intervals and at least annually. They shall update the assignment where necessary.	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
10.1.3	N/A	The relevant entities shall review the assignment of personnel to specific roles as referred to in point 1.2., as well as their commitment of human resources in that regard, at planned intervals and at least annually. They shall update the assignment where necessary.	Functional	intersects with	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	8	
10.2	Verification of background	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
10.2.1	N/A	The relevant entities shall ensure to the extent feasible verification of the background of their employees, and where applicable of direct suppliers and service providers in accordance with point 5.1.4, if necessary for their role, responsibilities and authorisations.	Functional	subset of	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	10	
10.2.1	N/A	The relevant entities shall ensure to the extent feasible verification of the background of their employees, and where applicable of direct suppliers and service providers in accordance with point 5.1.4, if necessary for their role, responsibilities and authorisations.	Functional	intersects with	Third-Party Personnel Security	HRS-10	Mechanisms exist to govern third-party personnel by reviewing and monitoring third-party cybersecurity & data privacy roles and responsibilities.	8	
10.2.1	N/A	The relevant entities shall ensure to the extent feasible verification of the background of their employees, and where applicable of direct suppliers and service providers in accordance with point 5.1.4, if necessary for their role, responsibilities and authorisations.	Functional	intersects with	Developer Screening	TDA-13	Mechanisms exist to ensure that the developers of systems, applications and/or services have the requisite skillset and appropriate access authorizations.	8	
10.2.1	N/A	The relevant entities shall ensure to the extent feasible verification of the background of their employees, and where applicable of direct suppliers and service providers in accordance with point 5.1.4, if necessary for their role, responsibilities and authorisations.	Functional	intersects with	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	8	
10.2.2	N/A	For the purpose of point 10.2.1., the relevant entities shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
10.2.2(a)	N/A	put in place criteria, which set out which roles, responsibilities and authorities shall only be exercised by persons whose background has been verified;	Functional	intersects with	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
10.2.2(b)	N/A	ensure that verification referred to in point 10.2.1 is performed on these persons before they start exercising these roles, responsibilities and authorities, which shall take into consideration the applicable laws, regulations, and ethics in proportion to the business requirements, the asset classification as referred to in point 12.1. and the network and information systems to be accessed, and the perceived risks.	Functional	intersects with	Personnel Screening	HRS-04	Mechanisms exist to manage personnel security risk by screening individuals prior to authorizing access.	5	
10.2.3	N/A	The relevant entities shall review and, where appropriate, update the policy at planned intervals and update it where necessary.	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
10.3	Termination or change of employment procedures	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
10.3.1	N/A	The relevant entities shall ensure that network and information system security responsibilities and duties that remain valid after termination or change of employment of their employees are contractually defined and enforced.	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	
10.3.1	N/A	The relevant entities shall ensure that network and information system security responsibilities and duties that remain valid after termination or change of employment of their employees are contractually defined and enforced.	Functional	intersects with	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
10.3.1	N/A	The relevant entities shall ensure that network and information system security responsibilities and duties that remain valid after termination or change of employment of their employees are contractually defined and enforced.	Functional	intersects with	Termination of Employment	IAC-07.2	Mechanisms exist to revoke user access rights in a timely manner, upon termination of employment or contract.	5	
10.3.2	N/A	For the purpose of point 10.3.1., the relevant entities shall include in the individual's terms and conditions of employment, contract or agreement the responsibilities and duties that are still valid after termination of employment or contract, such as confidentiality clauses.	Functional	intersects with	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity & data privacy principles in their daily work.	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 (optional)	Notes (optional)
10.3.2	N/A	For the purpose of point 10.3.1., the relevant entities shall include in the individual's terms and conditions of employment, contract or agreement the responsibilities and duties that are still valid after termination of employment or contract, such as confidentiality clauses.	Functional	intersects with	Confidentiality Agreements	HRS-06.1	Mechanisms exist to require Non-Disclosure Agreements (NDAs) or similar confidentiality agreements that reflect the needs to protect data and operational details, or both employees and third-parties.	8	
10.4	Disciplinary process	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
10.4.1	N/A	The relevant entities shall establish, communicate and maintain a disciplinary process for handling violations of network and information system security policies. The process shall take into consideration relevant legal, statutory, contractual and business requirements.	Functional	intersects with	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
10.4.1	N/A	The relevant entities shall establish, communicate and maintain a disciplinary process for handling violations of network and information system security policies. The process shall take into consideration relevant legal, statutory, contractual and business requirements.	Functional	intersects with	Workplace Investigations	HRS-07.1	Mechanisms exist to conduct employee misconduct investigations when there is reasonable assurance that a policy has been violated.	5	
10.4.2	N/A	The relevant entities shall review and, where appropriate, update the disciplinary process at planned intervals, and when necessary due to legal changes or significant changes to operations or risks.	Functional	equal	Updating Disciplinary Processes	HRS-07.2	Mechanisms exist to periodically review and, where appropriate, update disciplinary process(es) due to: (1) Legal changes; (2) Significant changes to operations; and (3) Applicable threats and risks.	10	
11	ACCESS CONTROL (ARTICLE 21(2), POINTS (I) AND (J), OF DIRECTIVE (EU) 2022/2555)	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
11.1	Access control policy	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
11.1.1	N/A	For the purpose of Article 21(2), point (i) of Directive (EU) 2022/2555, the relevant entities shall establish, document and implement logical and physical access control policies for the access to their network and information systems, based on business requirements as well as network and information system security requirements.	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
11.1.1	N/A	For the purpose of Article 21(2), point (i) of Directive (EU) 2022/2555, the relevant entities shall establish, document and implement logical and physical access control policies for the access to their network and information systems, based on business requirements as well as network and information system security requirements.	Functional	intersects with	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	8	
11.1.2	N/A	The policies referred to in point 11.1.1. shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
11.1.2(a)	N/A	address access by persons, including staff, visitors, and external entities such as suppliers and service providers;	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
11.1.2(b)	N/A	address access by network and information systems;	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
11.1.2(c)	N/A	ensure that access is only granted to users that have been adequately authenticated.	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
11.1.3	N/A	The relevant entities shall review and, where appropriate, update the policies at planned intervals and when significant incidents or significant changes to operations or risks occur.	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
11.2	Management of access rights	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
11.2.1	N/A	The relevant entities shall provide, modify, remove and document access rights to network and information systems in accordance with the access control policy referred to in point 11.1.	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	
11.2.2	N/A	The relevant entities shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
11.2.2(a)	N/A	assign and revoke access rights based on the principles of need-to-know, least privilege and separation of duties;	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	
11.2.2(a)	N/A	assign and revoke access rights based on the principles of need-to-know, least privilege and separation of duties;	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	
11.2.2(a)	N/A	assign and revoke access rights based on the principles of need-to-know, least privilege and separation of duties;	Functional	intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
11.2.2(a)	N/A	assign and revoke access rights based on the principles of need-to-know, least privilege and separation of duties;	Functional	intersects with	Revocation of Access Authorizations	IAC-20.6	Mechanisms exist to revoke logical and physical access authorizations.	5	
11.2.2(a)	N/A	assign and revoke access rights based on the principles of need-to-know, least privilege and separation of duties;	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	
11.2.2(b)	N/A	ensure that access rights are modified accordingly upon termination or change of employment;	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	
11.2.2(b)	N/A	ensure that access rights are modified accordingly upon termination or change of employment;	Functional	intersects with	Revocation of Access Authorizations	IAC-20.6	Mechanisms exist to revoke logical and physical access authorizations.	5	
11.2.2(c)	N/A	ensure that access to network and information systems is authorised by the relevant persons;	Functional	intersects with	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	10	
11.2.2(c)	N/A	ensure that access to network and information systems is authorised by the relevant persons;	Functional	intersects with	Management Approval For New or Changed Accounts	IAC-28.1	Mechanisms exist to ensure management approvals are required for new accounts or changes in permissions to existing accounts.	5	
11.2.2(d)	N/A	ensure that access rights appropriately address third-party access, such as visitors, suppliers and service providers, in particular by limiting access rights in scope and in duration;	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	
11.2.2(d)	N/A	ensure that access rights appropriately address third-party access, such as visitors, suppliers and service providers, in particular by limiting access rights in scope and in duration;	Functional	intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
11.2.2(d)	N/A	ensure that access rights appropriately address third-party access, such as visitors, suppliers and service providers, in particular by limiting access rights in scope and in duration;	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	
11.2.2(e)	N/A	maintain a register of access rights granted;	Functional	intersects with	User & Service Account Inventories	IAC-01.3	Automated mechanisms exist to maintain a current list of authorized users and service accounts.	5	
11.2.2(f)	N/A	apply logging to the management of access rights.	Functional	intersects with	Account Creation and Modification Logging	MON-16.4	Automated mechanisms exist to generate event logs for permissions changes to privileged accounts and/or groups.	5	
11.2.3	N/A	The relevant entities shall review access rights at planned intervals and shall modify them based on organisational changes. The relevant entities shall document the results of the review including the necessary changes of access rights.	Functional	intersects with	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	8	
11.3	Privileged accounts and system administration accounts	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
11.3.1	N/A	The relevant entities shall maintain policies for management of privileged accounts and system administration accounts as part of the access control policy referred to in point 11.1.	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
11.3.2	N/A	The policies referred to in point 11.3.1. shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
11.3.2(a)	N/A	establish strong identification, authentication such as multi-factor authentication, and authorisation procedures for privileged accounts and system administration accounts;	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	
11.3.2(a)	N/A	establish strong identification, authentication such as multi-factor authentication, and authorisation procedures for privileged accounts and system administration accounts;	Functional	intersects with	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	
11.3.2(b)	N/A	set up specific accounts to be used for system administration operations exclusively, such as installation, configuration, management or maintenance;	Functional	intersects with	Privileged Accounts	IAC-21.3	Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles.	5	
11.3.2(c)	N/A	individualise and restrict system administration privileges to the highest extent possible,	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	
11.3.2(d)	N/A	provide that system administration accounts are only used to connect to system administration systems.	Functional	intersects with	Dedicated Administrative Machines	IAC-20.4	Mechanisms exist to restrict executing administrative tasks or tasks requiring elevated access to a dedicated machine.	5	
11.3.2(d)	N/A	provide that system administration accounts are only used to connect to system administration systems.	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	
11.3.3	N/A	The relevant entities shall review access rights of privileged accounts and system administration accounts at planned intervals and be modified based on organisational changes, and shall document the results of the review, including the necessary changes of access rights.	Functional	intersects with	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
11.4	Administration systems	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
11.4.1	N/A	The relevant entities shall restrict and control the use of system administration systems in accordance with the access control policy referred to in point 11.1.	Functional	intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce a Role-Based Access Control (RBAC) policy over users and resources that applies need-to-know and fine-grained access control for sensitive/regulated data access.	5	
11.4.2	N/A	For that purpose, the relevant entities shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
11.4.2(a)	N/A	only use system administration systems for system administration purposes, and not for any other operations;	Functional	intersects with	Dedicated Administrative Machines	IAC-20.4	Mechanisms exist to restrict executing administrative tasks or tasks requiring elevated access to a dedicated machine.	8	
11.4.2(b)	N/A	separate logically such systems from application software not used for system administrative purposes,	Functional	intersects with	Process Isolation	SEA-04	Mechanisms exist to implement a separate execution domain for each executing process.	5	
11.4.2(c)	N/A	protect access to system administration systems through authentication and encryption.	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	
11.4.2(c)	N/A	protect access to system administration systems through authentication and encryption.	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.	5	
11.5	Identification	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
11.5.1	N/A	The relevant entities shall manage the full life cycle of identities of network and information systems and their users.	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
11.5.2	N/A	For that purpose, the relevant entities shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
11.5.2(a)	N/A	set up unique identities for network and information systems and their users;	Functional	intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
11.5.2(a)	N/A	set up unique identities for network and information systems and their users;	Functional	intersects with	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5	
11.5.2(b)	N/A	link the identity of users to a single person;	Functional	intersects with	User Identity (ID) Management	IAC-09.1	Mechanisms exist to ensure proper user identification management for non-consumer users and administrators.	5	
11.5.2(b)	N/A	link the identity of users to a single person;	Functional	intersects with	Audit Trails	MON-03.2	Mechanisms exist to link system access to individual users or service accounts.	5	
11.5.2(c)	N/A	ensure oversight of identities of network and information systems;	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
11.5.2(c)	N/A	ensure oversight of identities of network and information systems;	Functional	intersects with	Account Management	IAC-15	Mechanisms exist to proactively govern account management of individual, group, system, service, application, guest and temporary accounts.	8	
11.5.2(d)	N/A	apply logging to the management of identities.	Functional	intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure systems 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	
11.5.2(d)	N/A	apply logging to the management of identities.	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	
11.5.3	N/A	The relevant entities shall only permit identities assigned to multiple persons, such as shared identities, where they are necessary for business or operational reasons and are subject to an explicit approval process and documentation. The relevant entities shall take identities assigned to multiple persons into account in the cybersecurity risk management framework referred to in point 2.1.	Functional	intersects with	Restrictions on Shared Groups / Accounts	IAC-15.5	Mechanisms exist to authorize the use of shared/group accounts only under certain organization-defined conditions.	5	
11.5.4	N/A	The relevant entities shall regularly review the identities for network and information systems and their users and, if no longer needed, deactivate them without delay.	Functional	intersects with	Periodic Review of Account Privileges	IAC-17	Mechanisms exist to periodically-review the privileges assigned to individuals and service accounts to validate the need for such privileges and reassign or remove unnecessary privileges, as necessary.	5	
11.6	Authentication	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
11.6.1	N/A	The relevant entities shall implement secure authentication procedures and technologies based on access restrictions and the policy on access control.	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	
11.6.2	N/A	For that purpose, the relevant entities shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
11.6.2(a)	N/A	ensure the strength of authentication is appropriate to the classification of the asset to be accessed;	Functional	subset of	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	10	
11.6.2(b)	N/A	control the allocation to users and management of secret authentication information by a process that ensures the confidentiality of the information, including advising personnel on appropriate handling of authentication information;	Functional	intersects with	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
11.6.2(c)	N/A	require the change of authentication credentials initially, at predefined intervals and upon suspicion that the credentials were compromised;	Functional	intersects with	Events Requiring Authenticator Change	IAC-10.13	Mechanisms exist to change authentication credentials: (1) At predefined intervals; and/or (2) Upon suspicion of credential compromise.	5	
11.6.2(d)	N/A	require the reset of authentication credentials and the blocking of users after a predefined number of unsuccessful log-in attempts;	Functional	intersects with	Account Lockout	IAC-22	Mechanisms exist to enforce a limit for consecutive invalid login attempts by a user during an organization-defined time period and automatically locks the account when the maximum number of unsuccessful attempts is exceeded.	5	
11.6.2(e)	N/A	terminate inactive sessions after a predefined period of inactivity; and	Functional	intersects with	Session Termination	IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	5	
11.6.2(f)	N/A	require separate credentials to access privileged access or administrative accounts.	Functional	subset of	Privileged Account Management (PAM)	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and services.	10	
11.6.3	N/A	The relevant entities shall to the extent feasible use state-of-the-art authentication methods, in accordance with the associated assessed risk and the classification of the asset to be accessed, and unique authentication information.	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	
11.6.4	N/A	The relevant entities shall review the authentication procedures and technologies at planned intervals.	Functional	subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
11.7	Multi-factor authentication	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
11.7.1	N/A	The relevant entities shall ensure that users are authenticated by multiple authentication factors or continuous authentication mechanisms for accessing the relevant entities' network and information systems, where appropriate, in accordance with the classification of the asset to be accessed.	Functional	intersects with	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party systems, applications and/or services; and/ or (3) Non-console access to critical systems or systems that store, transmit and/or process sensitive/regulated data.	5	
11.7.1	N/A	The relevant entities shall ensure that users are authenticated by multiple authentication factors or continuous authentication mechanisms for accessing the relevant entities' network and information systems, where appropriate, in accordance with the classification of the asset to be accessed.	Functional	intersects with	Continuous Authentication	IAC-13.3	Automated mechanisms exist to enable continuous re-authentication through the lifecycle of entity interactions.	5	
11.7.2	N/A	The relevant entities shall ensure that the strength of authentication is appropriate for the classification of the asset to be accessed.	Functional	intersects with	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity & data privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all systems, applications, services and personnel (internal and third-parties).	3	
11.7.2	N/A	The relevant entities shall ensure that the strength of authentication is appropriate for the classification of the asset to be accessed.	Functional	intersects with	Authenticator Management	IAC-10	Mechanisms exist to: (1) Securely manage authenticators for users and devices; and (2) Ensure the strength of authentication is appropriate to the classification of the data being accessed.	5	
12	ASSET MANAGEMENT (ARTICLE 21(2), POINT (I), OF DIRECTIVE (EU) 2022/2555)	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
12.1	Asset classification	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
12.1.1	N/A	For the purpose of Article 21(2), point (i) of Directive (EU) 2022/2555, the relevant entities shall lay down classification levels of all assets, including information, in scope of their network and information systems for the level of protection required.	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	
12.1.1	N/A	For the purpose of Article 21(2), point (i) of Directive (EU) 2022/2555, the relevant entities shall lay down classification levels of all assets, including information, in scope of their network and information systems for the level of protection required.	Functional	intersects with	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity & data privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all systems, applications, services and personnel (internal and third-parties).	3	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
12.1.1	N/A	For the purpose of Article 21(2), point (i) of Directive (EU) 2022/2555, the relevant entities shall lay down classification levels of all assets, including information, in scope of their network and information systems for the level of protection required.	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	
12.1.2	N/A	For the purpose of point 12.1.1., the relevant entities shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
12.1.2(a)	N/A	lay down a system of classification levels for assets;	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.	8	
12.1.2(b)	N/A	associate all assets with a classification level, based on confidentiality, integrity, authenticity and availability requirements, to indicate the protection required according to their sensitivity, criticality, risk and business value;	Functional	intersects with	Highest Classification Level	DCH-02.1	Mechanisms exist to ensure that systems, applications and services are classified according to the highest level of data sensitivity that is stored, transmitted and/or processed.	5	
12.1.2(c)	N/A	align the availability requirements of the assets with the delivery and recovery objectives set out in their business continuity and disaster recovery plans.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
12.1.3	N/A	The relevant entities shall conduct periodic reviews of the classification levels of assets and update them, where appropriate.	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	
12.1.3	N/A	The relevant entities shall conduct periodic reviews of the classification levels of assets and update them, where appropriate.	Functional	intersects with	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity & data privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all systems, applications, services and personnel (internal and third-parties).	5	
12.2	Handling of assets	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
12.2.1	N/A	The relevant entities shall establish, implement and apply a policy for the proper handling of assets, including information, in accordance with their network and information security policy, and shall communicate the policy on proper handling of assets to anyone who uses or handles assets.	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	
12.2.2	N/A	The policy shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
12.2.2(a)	N/A	cover the entire life cycle of the assets, including acquisition, use, storage, transportation and disposal;	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	
12.2.2(b)	N/A	provide rules on the safe use, safe storage, safe transport, and the irretrievable deletion and destruction of the assets;	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.	5	
12.2.2(c)	N/A	provide that the transfer shall take place in a secure manner, in accordance with the type of asset to be transferred.	Functional	intersects with	Security of Assets & Media	AST-05	Mechanisms exist to maintain strict control over the internal or external distribution of any kind of sensitive/regulated media.	3	
12.2.3	N/A	The relevant entities shall review and, where appropriate, update the policy at planned intervals and when significant incidents or significant changes to operations or risks occur.	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	
12.3	Removable media policy	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
12.3.1	N/A	The relevant entities shall establish, implement and apply a policy on the management of removable storage media and communicate it to their employees and third parties who handle removable storage media at the relevant entities' premises or other locations where the removable media is connected to the relevant entities' network and information systems.	Functional	intersects with	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5	
12.3.2	N/A	The policy shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
12.3.2(a)	N/A	provide for a technical prohibition of the connection of removable media unless there is an organisational reason for their use;	Functional	intersects with	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5	
12.3.2(b)	N/A	provide for disabling self-execution from such media and scanning the media for malicious code before they are used on the relevant entities' systems;	Functional	subset of	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	10	
12.3.2(c)	N/A	provide measures for controlling and protecting portable storage devices containing data while in transit and in storage;	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	
12.3.2(c)	N/A	provide measures for controlling and protecting portable storage devices containing data while in transit and in storage;	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.	5	
12.3.2(d)	N/A	where appropriate, provide measures for the use of cryptographic techniques to protect data on removable storage media.	Functional	intersects with	Removable Media Security	DCH-12	Mechanisms exist to restrict removable media in accordance with data handling and acceptable usage parameters.	5	
12.3.3	N/A	The relevant entities shall review and, where appropriate, update the policy at planned intervals and when significant incidents or significant changes to operations or risks occur.	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	
12.4	Asset inventory	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
12.4.1	N/A	The relevant entities shall develop and maintain a complete, accurate, up-to-date and consistent inventory of their assets. They shall record changes to the entries in the inventory in a traceable manner.	Functional	subset of	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services 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	
12.4.2	N/A	The granularity of the inventory of the assets shall be at a level appropriate for the needs of the relevant entities. The inventory shall include the following:	Functional	subset of	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services 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	
12.4.2(a)	N/A	the list of operations and services and their description,	Functional	subset of	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services 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	
12.4.2(a)	N/A	the list of operations and services and their description,	Functional	intersects with	Compliance-Specific Asset Identification	AST-04.3	Mechanisms exist to create and maintain a current inventory of systems, applications and services that are in scope for statutory, regulatory and/or contractual compliance obligations that provides sufficient detail to determine control applicability, based on asset scope categorization.	5	
12.4.2(b)	N/A	the list of network and information systems and other associated assets supporting the relevant entities' operations and services.	Functional	subset of	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services 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	
12.4.2(b)	N/A	the list of network and information systems and other associated assets supporting the relevant entities' operations and services.	Functional	intersects with	Compliance-Specific Asset Identification	AST-04.3	Mechanisms exist to create and maintain a current inventory of systems, applications and services that are in scope for statutory, regulatory and/or contractual compliance obligations that provides sufficient detail to determine control applicability, based on asset scope categorization.	5	
12.4.3	N/A	The relevant entities shall regularly review and update the inventory and their assets and document the history of changes.	Functional	intersects with	Updates During Installations / Removals	AST-02.1	Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
12.5	Deposit, return or deletion of assets upon termination of employment	The relevant entities shall establish, implement and apply procedures which ensure that their assets which are under custody of personnel are deposited, returned or deleted upon termination of employment, and shall document the deposit, return and deletion of those assets. Where the deposit, return or deletion of assets is not possible, the relevant entities shall ensure that the assets can no longer access the relevant entities' network and information systems in accordance with point 12.2.2.	Functional	intersects with	Personnel Termination	HRS-09	Mechanisms exist to govern the termination of individual employment.	5	
12.5	Deposit, return or deletion of assets upon termination of employment	The relevant entities shall establish, implement and apply procedures which ensure that their assets which are under custody of personnel are deposited, returned or deleted upon termination of employment, and shall document the deposit, return and deletion of those assets. Where the deposit, return or deletion of assets is not possible, the relevant entities shall ensure that the assets can no longer access the relevant entities' network and information systems in accordance with point 12.2.2.	Functional	intersects with	Asset Collection	HRS-09.1	Mechanisms exist to retrieve organization-owned assets upon termination of an individual's employment.	5	
13	ENVIRONMENTAL AND PHYSICAL SECURITY (ARTICLE 21(2), POINTS (C), (E) AND (I) OF DIRECTIVE (EU) 2022/2555)	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
13.1	Supporting utilities	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
13.1.1	N/A	For the purpose of Article 21(2)(c) of Directive (EU) 2022/2555, the relevant entities shall prevent loss, damage or compromise of network and information systems or interruption to their operations due to the failure and disruption of supporting utilities.	Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
13.1.2	N/A	For that purpose, the relevant entities shall, where appropriate:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
13.1.2(a)	N/A	protect facilities from power failures and other disruptions caused by failures in supporting utilities such as electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning;	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.	5	
13.1.2(a)	N/A	protect facilities from power failures and other disruptions caused by failures in supporting utilities such as electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning;	Functional	intersects with	Emergency Lighting	PES-07.4	Facility security mechanisms exist to utilize and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	5	
13.1.2(b)	N/A	consider the use of redundancy in utilities services;	Functional	intersects with	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover system, which is not collocated with the primary system, application and/or service, which can be activated with little-to-no loss of information or disruption to operations.	5	
13.1.2(c)	N/A	protect utility services for electricity and telecommunications, which transport data or supply network and information systems, against interception and damage;	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	
13.1.2(d)	N/A	monitor the utility services referred to in point (c) and report to the competent internal or external personnel events outside the minimum and maximum control thresholds referred to in point 13.2.2(b) affecting the utility services;	Functional	intersects with	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
13.1.2(d)	N/A	monitor the utility services referred to in point (c) and report to the competent internal or external personnel events outside the minimum and maximum control thresholds referred to in point 13.2.2(b) affecting the utility services;	Functional	intersects with	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	5	
13.1.2(e)	N/A	conclude contracts for the emergency supply with corresponding services, such as for the fuel for emergency power supply;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
13.1.2(f)	N/A	ensure continuous effectiveness, monitor, maintain and test the supply of the network and information systems necessary for the operation of the service offered, in particular the electricity, temperature and humidity control, telecommunications and Internet connection.	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
13.1.2(f)	N/A	ensure continuous effectiveness, monitor, maintain and test the supply of the network and information systems necessary for the operation of the service offered, in particular the electricity, temperature and humidity control, telecommunications and Internet connection.	Functional	intersects with	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	8	
13.1.2(f)	N/A	ensure continuous effectiveness, monitor, maintain and test the supply of the network and information systems necessary for the operation of the service offered, in particular the electricity, temperature and humidity control, telecommunications and Internet connection.	Functional	intersects with	Temperature & Humidity Controls	PES-09	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	5	
13.1.3	N/A	The relevant entities shall test, review and, where appropriate, update the protection measures on a regular basis or following significant incidents or significant changes to operations or risks.	Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
13.2	Protection against physical and environmental threats	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
13.2.1	N/A	For the purpose of Article 21(2)(e) of Directive (EU) 2022/2555, the relevant entities shall prevent or reduce the consequences of events originating from physical and environmental threats, such as natural disasters and other intentional or unintentional threats, based on the results of the risk assessment carried out pursuant to point 2.1.	Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
13.2.1	N/A	For the purpose of Article 21(2)(e) of Directive (EU) 2022/2555, the relevant entities shall prevent or reduce the consequences of events originating from physical and environmental threats, such as natural disasters and other intentional or unintentional threats, based on the results of the risk assessment carried out pursuant to point 2.1.	Functional	intersects with	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	8	
13.2.2	N/A	For that purpose, the relevant entities shall, where appropriate:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
13.2.2(a)	N/A	design and implement protection measures against physical and environmental threats;	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	8	
13.2.2(a)	N/A	design and implement protection measures against physical and environmental threats;	Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
13.2.2(b)	N/A	determine minimum and maximum control thresholds for physical and environmental threats;	Functional	intersects with	Risk Threshold	RSK-01.4	Mechanisms exist to define organizational risk threshold, the level of risk exposure above which risks are addressed and below which risks may be accepted.	8	
13.2.2(c)	N/A	monitor environmental parameters and report to the competent internal or external personnel events outside the minimum and maximum control thresholds referred to in point (b).	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
13.2.2(c)	N/A	monitor environmental parameters and report to the competent internal or external personnel events outside the minimum and maximum control thresholds referred to in point (b).	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
13.2.3	N/A	The relevant entities shall test, review and, where appropriate, update the protection measures against physical and environmental threats on a regular basis or following significant incidents or significant changes to operations or risks.	Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
13.3	Perimeter and physical access control	N/A	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
13.3.1	N/A	For the purpose of Article 21(2)(i) of Directive (EU) 2022/2555, the relevant entities shall prevent and monitor unauthorised physical access, damage and interference to their network and information systems.	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	
13.3.1	N/A	For the purpose of Article 21(2)(i) of Directive (EU) 2022/2555, the relevant entities shall prevent and monitor unauthorised physical access, damage and interference to their network and information systems.	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	
13.3.2	N/A	For that purpose, the relevant entities shall:	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
13.3.2(a)	N/A	on the basis of the risk assessment carried out pursuant to point 2.1, lay down and use security perimeters to protect areas where network and information systems and other associated assets are located;	Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
13.3.2(b)	N/A	protect the areas referred to in point (a) by appropriate entry controls and access points;	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	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
13.3.2(b)	N/A	protect the areas referred to in point (a) by appropriate entry controls and access points;	Functional	intersects with	Controlled Ingress & Egress Points	PES-03.1	Physical access control mechanisms exist to limit and monitor physical access through controlled ingress and egress points.	5	
13.3.2(c)	N/A	design and implement physical security for offices, rooms and facilities,	Functional	intersects with	Physical Security of Offices, Rooms & Facilities	PES-04	Mechanisms exist to identify systems, equipment and respective operating environments that require limited physical access so that appropriate physical access controls are designed and implemented for offices, rooms and facilities.	5	
13.3.2(d)	N/A	continuously monitor their premises for unauthorised physical access.	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	
13.3.2(d)	N/A	continuously monitor their premises for unauthorised physical access.	Functional	intersects with	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	
13.3.3	N/A	The relevant entities shall test, review and, where appropriate, update the physical access control measures on a regular basis or following significant incidents or significant changes to operations or risks.	Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	