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-

EU NIS2 Directive

Focal Document: European Union (EU) NIS2 Directive
Focal Document URL: https://www.foca.uropa.au/legal-content/EU/TXT/PDF/Pr/uri-CELEX/2022L2555-2022127Aqd-1734387542792
Published STRM URL: https://www.com/content/EU/TXT/PDF/Pr/uri-CELEX/2022L2555-2022127Aqd-1734387542792
https://www.com/content/EU/TXT/PDF/Pr/uri-CELEX/2022L2555-2022127Aqd-1734387542792

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)
Article 21.1	N/A	Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and no other services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subgangings that enumes a level of security of reflexor in deviational standards, as well as the cost of implementation, the measures referred to in the first subgangings that enumes a level of security of reflexor deviationally of those resources, the count shall be taken of the degree of the entity's sepouter to frisk, the entity's size and the literations of occurrence of incidents and their severity, including their societal and economic impact.	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
Article 21.1	N/A	Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities used to their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and no other services. Taking into account the state of -the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subgragage that learness a level of security of retwork and information systems appropriate to the that speed, of the assessing the proportionally of those the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.	Functional	intersects with	Cybersecurity & Data Protection Assessments	CPL-03	Mechanisms exist to regularly review processes and documented procedures to ensure conformity with the organization's cybersacurity & data protection policies, standards and other applicable requirements.	5	
Article 21.1	N/A	Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entitles use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and no other services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subgragged shall ensure a level of security of reflexor flat ending the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subgragged shall ensure a level of security of reflexor flat endings of the security application of researching the security of the degree of the entity's apposant or to first, the entity's size and the likelihood of occurrence of incidents and their sevenity, studient (their occurrence of insignat.	Functional	intersects with	Functional Review Of Cybersecurily & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity & data protection policies and standards.	5	
Article 21.1	N/A	Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risk posed to the security of network and information systems which those entities or their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and not prevent or minimise the impact of microlians to recipients of their services and not prevent or minimise the impact of microlians or recipients of their services and not prevent or minimise the impact of microlians or recipients of their services and not prevent or services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subgragage shall all ensure a level of security of retenvice and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the mitty's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their solvidant and economic impact.	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Machaniams exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
Article 21.1	N/A	Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entitles or their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and no other services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subgrage pits hall ensure a level of security of reterors and international standards, as well as the cost of implementation, the measures referred to systems appropriate to the risks posed. When assessing the proportionality of those measures, the account shall be taken of the degree of the entity's acposure to risks, the entity's size and the literations of occurrence of incidents and their seventy, including their societal and economic impact.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 21.1	N/A	Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities or their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and no other services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subgrage pits hall ensure a level of security of reterois and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's acposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their soloidal and economic impact.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compet data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
Article 21.1	N/A	Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risk posed to the security of network and information systems which those entities used to their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and not other services. Taking into account the state-of-the-ort and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subgragging shall an enternal as level of security of reflects and continuous subgragging shall are as level of security of reflects and continuous subgragging shall are used to the state-of-the-ort and in the state-of-the-ort and the sta	Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compet data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
Article 21.1	N/A	Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for the operation or for the provision of the services, and to operate or minimums the impact of incidents on recipients of their services and on other services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of the measures, due account shall be taken of the degree of the entity's is exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.	Functional	intersects with	Implement Controls	GOV-15.2	Mechaniams exist to compel data and/or process owners to implement required cyber security & data privacy controls for each system, application and/or service under their control.	5	
Article 21.1	N/A	Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the ecurity of network and information systems which those entities or their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. The services and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionally for the onesaures, due account shall be taken of the degree of the entity's exposure to risks, the entity's as and the likelihood of ouccurrace of incidents and their severity, including their societal and economic impact.	Functional	intersects with	Risk Management Program	RSK-01	Machaniama exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	

Secure Controls Framework (SCF)

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		Member States shall ensure that essential and important entities take appropriate and					Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure,	(optional)	
		proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for					disruption, modification or destruction of the organization's systems and data.		
		their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.							
Article 21.1	N/A	Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred	Functional	intersects with	Risk Assessment	RSK-04		5	
		to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks,							
		the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.							
		Member States shall ensure that essential and important entities take appropriate and					Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development,		
		proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for					implementation and modification of systems and services.		
		their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.							
Article 21.1	N/A	Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred	Functional	intersects with	Secure Engineering Principles	SEA-01		5	
		to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks,							
		the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.							
Article 21.2	N/A	The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of	Functional	subset of	Cybersecurity & Data Protection Governance	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
		those systems from incidents, and shall include at least the following:			Program Cybersecurity & Data		Mechanisms exist to facilitate the implementation of cybersecurity & data protection		
Article 21.2(a)	N/A	policies on risk analysis and information system security;	Functional	subset of	Protection Governance Program	GOV-01	governance controls.  Mechanisms exist to establish, maintain and disseminate cybersecurity & data	10	
Article 21.2(a)	N/A	policies on risk analysis and information system security;	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	protection policies, standards and procedures.	5	
Article 21.2(a)	N/A	policies on risk analysis and information system security;	Functional	intersects with	Operationalizing Cybersecurity & Data	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service	5	
					Protection Practices		under their control.  Mechanisms exist to compel data and/or process owners to select required		
Article 21.2(a)	N/A	policies on risk analysis and information system security;	Functional	intersects with	Select Controls	GOV-15.1	cybersecurity & data privacy controls for each system, application and/or service under their control.  Mechanisms exist to compel data and/or process owners to implement required	5	
Article 21.2(a)	N/A	policies on risk analysis and information system security;	Functional	intersects with	Implement Controls	GOV-15.2	cybersecurity & data privacy controls for each system, application and/or service under their control.  Mechanisms exist to facilitate the implementation of strategic, operational and	5	
Article 21.2(a)	N/A	policies on risk analysis and information system security;	Functional	intersects with	Risk Management Program Cybersecurity & Data	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.  Mechanisms exist to facilitate the implementation of cybersecurity & data protection	5	
Article 21.2(b)	N/A	incident handling;	Functional	subset of	Protection Governance Program	GOV-01	governance controls.  Mechanisms exist to establish, maintain and disseminate cybersecurity & data	10	
Article 21.2(b)	N/A	incident handling:	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	protection policies, standards and procedures.	5	
Article 21.2(b)	N/A	incident handling;	Functional	intersects with	Operationalizing Cybersecurity & Data	GOV-15	Mechanisms exist to compet data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service	5	
Article 21.2(b)	N/A	incident handling:	Functional	intersects with	Protection Practices Select Controls		under their control.  Mechanisms exist to compel data and/or process owners to select required	5	
		-					cybersecurity & data privacy controls for each system, application and/or service under their control.  Mechanisms exist to compel data and/or process owners to implement required		
Article 21.2(b)	N/A	incident handling:	Functional	intersects with	Implement Controls	GOV-15.2	cybersecurity & data privacy controls for each system, application and/or service <u>under their control</u> .  Mechanisms exist to implement and govern processes and documentation to	5	
Article 21.2(b)	N/A	incident handling:	Functional	intersects with	Incident Response Operations	IRO-01	facilitate an organization-wide response capability for cybersecurity & data privacy- related incidents.	5	
							Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake;		
Article 21.2(b)	N/A	incident handling;	Functional	intersects with	Incident Handling	IRO-02	(3) Analysis; (4) Containment;	5	
					Business Continuity		(5) Eradication; and  (6) Recovery  Mechanisms exist to facilitate the implementation of contingency planning controls		
Article 21.2(c)	N/A	business continuity, such as backup management and disaster recovery, and crisis management;	Functional	subset of	Management System (BCMS)	BCD-01	to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
Article 21.2(c)	N/A	business continuity, such as backup management and disaster recovery, and crisis	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	5	
		management;  business continuity, such as backup management and disaster recovery, and crisis			Information System		the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). Mechanisms exist to ensure the secure recovery and reconstitution of systems to a		
Article 21.2(c)	N/A	management;	Functional	intersects with	Recovery & Reconstitution Cybersecurity & Data	BCD-12	known state after a disruption, compromise or failure.  Mechanisms exist to facilitate the implementation of cybersecurity & data protection	5	
Article 21.2(c)	N/A	business continuity, such as backup management and disaster recovery, and crisis management;	Functional	subset of	Protection Governance Program	GOV-01	governance controls.	10	
Article 21.2(c)	N/A	business continuity, such as backup management and disaster recovery, and crisis management;	Functional	intersects with	Publishing Cybersecurity & Data Protection	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 21.2(c)	N/A	business continuity, such as backup management and disaster recovery, and crisis	Functional	intersects with	Operationalizing Cybersecurity & Data	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service	5	
		management; business continuity, such as backup management and disaster recovery, and crisis			Protection Practices		under their control.  Mechanisms exist to compel data and/or process owners to select required		
Article 21.2(c)	N/A	management;	Functional	intersects with	Select Controls		cybersecurity & data privacy controls for each system, application and/or service under their control.  Mechanisms exist to compel data and/or process owners to implement required	5	
Article 21.2(c)	N/A	business continuity, such as backup management and disaster recovery, and crisis management;	Functional	intersects with	Implement Controls	GOV-15.2	cybersecurity & data privacy controls for each system, application and/or service under their control.  Mechanisms exist to facilitate the implementation of cybersecurity & data protection	5	
Article 21.2(d)	N/A	supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	governance controls.	10	
Article 21.2(d)	N/A	supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;	Functional	intersects with	Publishing Cybersecurity & Data Protection	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Application Cod Trim	****	supply chain security, including security-related aspects concerning the relationships	Europeio :	inter	Operationalizing	001:-	Mechanisms exist to compel data and/or process owners to operationalize	-	
Article 21.2(d)	N/A	between each entity and its direct suppliers or service providers; supply chain security, including security-related aspects concerning the relationships	Functional	intersects with	Cybersecurity & Data Protection Practices		cybersecurity & data privacy practices for each system, application and/or service under their control.  Mechanisms exist to compel data and/or process owners to select required	5	
Article 21.2(d)	N/A	between each entity and its direct suppliers or service providers;	Functional	intersects with	Select Controls	GOV-15.1	cybersecurity & data privacy controls for each system, application and/or service under their control.  Mechanisms exist to compel data and/or process owners to implement required	5	
Article 21.2(d)	N/A	supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;	Functional	intersects with	Implement Controls		cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
Article 21.2(d)	N/A	supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;	Functional	intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.  Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM)	5	
Article 21.2(d)	N/A	supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	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	
Article 21.2(d)	N/A	supply chain security, including security-related aspects concerning the relationships	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management	5	
		between each entity and its direct suppliers or service providers;					controls.  Mechanisms exist to: (1) Evaluate security risks and threats associated with the services and product		
Article 21.2(d)	N/A	supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;	Functional	intersects with	Supply Chain Risk Management (SCRM)	TPM-03	supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to	5	
Article 21.2(e)	N/A	security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	Functional	subset of	Cybersecurity & Data Protection Governance	GOV-01	those risks and threats, as necessary.  Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
<u> </u>		monday randomy nandmy n			Program			<u> </u>	1



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
Article 21.2(e)	N/A	security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	Functional	intersects with	Publishing Cybersecurity & Data Protection	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	(optional) 5	
Article 21.2(e)	N/A	security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	Functional	intersects with	Operationalizing Cybersecurity & Data	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service	5	
Article 21.2(e)	N/A	security in network and information systems acquisition, development and	Functional	intersects with	Protection Practices  Select Controls	GOV-15.1	under their control.  Mechanisms exist to compel data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service	5	
Article 21.2(e)	N/A	maintenance, including vulnerability handling and disclosure; security in network and information systems acquisition, development and	Functional	intersects with	Implement Controls		under their control.  Mechanisms exist to compel data and/or process owners to implement required cybersecurity & data privacy controls for each system, application and/or service	5	
Article 21.2(e)	N/A	maintenance, including vulnerability handling and disclosure; security in network and information systems acquisition, development and	Functional	intersects with	Maintenance Operations	MNT-01	under their control.  Mechanisms exist to develop, disseminate, review & update procedures to facilitate	5	
Article 21.2(e)	N/A	maintenance, including vulnerability handling and disclosure; security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	Functional	intersects with	Network Security Controls (NSC)	NET-01	the implementation of maintenance controls across the enterprise.  Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	
Article 21.2(e)	N/A	security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	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	
Article 21.2(e)	N/A	security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	Functional	intersects with	Third-Party Management Vulnerability & Patch	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.  Mechanisms exist to facilitate the implementation and monitoring of vulnerability	5	
Article 21.2(e)	N/A	security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	Functional	intersects with	Management Program (VPMP) Cybersecurity & Data	VPM-01	management controls.	5	
Article 21.2(f)	N/A	policies and procedures to assess the effectiveness of cybersecurity risk- management measures;	Functional	subset of	Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
Article 21.2(f)	N/A	policies and procedures to assess the effectiveness of cybersecurity risk-management measures;	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
Article 21.2(f)	N/A	policies and procedures to assess the effectiveness of cybersecurity risk- management measures;	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 21.2(f)	N/A	policies and procedures to assess the effectiveness of cybersecurity risk- management measures;	Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
Article 21.2(f)	N/A	policies and procedures to assess the effectiveness of cybersecurity risk- management measures;	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.	5	
Article 21.2(f)	N/A	policies and procedures to assess the effectiveness of cybersecurity risk- management measures;	Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
Article 21.2(f)	N/A	policies and procedures to assess the effectiveness of cybersecurity risk- management measures;	Functional	intersects with	Implement Controls	GOV-15.2	Mechanisms exist to compet data and/or process owners to implement required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
Article 21.2(f)	N/A	policies and procedures to assess the effectiveness of cybersecurity risk- management measures;	Functional	intersects with	Risk Management Program Cybersecurity & Data	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.  Mechanisms exist to facilitate the implementation of cybersecurity & data protection	5	
Article 21.2(g)	N/A	basic cyber hygiene practices and cybersecurity training;	Functional	subset of	Protection Governance Program	GOV-01	governance controls.  Mechanisms exist to establish, maintain and disseminate cybersecurity & data	10	
Article 21.2(g)	N/A	basic cyber hygiene practices and cybersecurity training;	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	protection policies, standards and procedures.	5	
Article 21.2(g)	N/A	basic cyber hygiene practices and cybersecurity training;	Functional	intersects with	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.	5	
Article 21.2(g)	N/A	basic cyber hygiene practices and cybersecurity training;	Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compet data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
Article 21.2(g)	N/A	basic cyber hygiene practices and cybersecurity training:	Functional	intersects with	Implement Controls	GOV-15.2	Mechanisms exist to compet data and/or process owners to implement required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
Article 21.2(g)	N/A	basic cyber hygiene practices and cybersecurity training;	Functional	intersects with	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	5	
Article 21.2(h)	N/A	policies and procedures regarding the use of cryptography and, where appropriate, encryption;	Functional	intersects with	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
Article 21.2(h)	N/A	policies and procedures regarding the use of cryptography and, where appropriate, encryption;	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
Article 21.2(h)	N/A	policies and procedures regarding the use of cryptography and, where appropriate, encryption;	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 21.2(h)	N/A	policies and procedures regarding the use of cryptography and, where appropriate, encryption;	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.	5	
Article 21.2(h)	N/A	policies and procedures regarding the use of cryptography and, where appropriate, encryption;	Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service	5	
Article 21.2(h)	N/A	policies and procedures regarding the use of cryptography and, where appropriate, encryption;	Functional	intersects with	Implement Controls	GOV-15.2	under their control.  Mechanisms exist to compel data and/or process owners to implement required cybersecurity & data privacy controls for each system, application and/or service	5	
Article 21.2(i)	N/A	human resources security, access control policies and asset management;	Functional	intersects with	Asset Governance	AST-01	under their control.  Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
							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;		
Article 21.2(i)	N/A	human resources security, access control policies and asset management;	Functional	intersects with	Asset Inventories	AST-02	(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	
					Cuharoacurity & Data		(5) Is available for review and audit by designated organizational personnel.		
Article 21.2(i)	N/A	human resources security, access control policies and asset management;	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.  Mechanisms exist to establish majorais and discominate exhance with E data.	10	
Article 21.2(i)	N/A	human resources security, access control policies and asset management;	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 21.2(i)	N/A	human resources security, access control policies and asset management;	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.	5	
Article 21.2(i)	N/A	human resources security, access control policies and asset management;	Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
Article 21.2(i)	N/A	human resources security, access control policies and asset management;	Functional	intersects with	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
Article 21.2(i)	N/A	human resources security, access control policies and asset management;	Functional	intersects with	Human Resources Security Management Identity & Access	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.  Mechanisms exist to facilitate the implementation of identification and access	5	
Article 21.2(i)	N/A	human resources security, access control policies and asset management; the use of multi-factor authentication or continuous authentication solutions, secured	Functional	intersects with	Management (IAM) Cybersecurity & Data	IAC-01	management controls.  Mechanisms exist to facilitate the implementation of cybersecurity & data protection	5	
Article 21.2(j)	N/A	voice, video and text communications and secured emergency communication systems within the entity, where appropriate. the use of multi-factor authentication or continuous authentication solutions, secured	Functional	subset of	Protection Governance Program Publishing Cybersecurity	GOV-01	governance controls.  Mechanisms exist to establish, maintain and disseminate cybersecurity & data	10	
Article 21.2(j)	N/A	voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	Functional	intersects with	& Data Protection  Documentation	GOV-02	protection policies, standards and procedures.	5	
Article 21.2(j)	N/A	the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	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.	5	
Article 21.2(j)	N/A	the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
Article 21.2(j)	N/A	the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication	Functional	intersects with	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required cybersecurity & data privacy controls for each system, application and/or service	5	
Article 21.2(j)	N/A	systems within the entity, where appropriate.  the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication	Functional	intersects with	Identity & Access Management (IAM)	IAC-01	under their control.  Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
		systems within the entity, where appropriate.	1	1	management (IAM)	L			



FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
Article 21.2(j)	N/A	the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	Functional	intersects with	Multi-Factor Authentication (MFA)	IAC-06	Automated mechanisms exist to enforce httls-factor Authentication (MFA) for: (1) Remote network access; (2) Tind-party spitesses, applications and/or services; and/or (3) Non-console access to critical systems or systems that store, transmit and/or process sentative-regulated data.	(optional) 5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are apportine, entities take into account the vulnerabilities people to each first supplier and service provider and the overall quality of products and operaccurity practices of their suppliers and service providers, including their secure development procedures. Permiser States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 2211.	Functional	intersects with	Cybersecurity & Data Privacy in Project Management	PRM-04	Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures retired to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vurinerabilities specific to each direct supplier and service provider and the overall quality of products and operacurity practices of their suppliers and service providers, including their secure development procedures. Permiser States shall also ensure that, when considering which measures referred to in that point are appropriate, entries are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 2211.	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	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (i), of this Article are appropriate, entitles take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and ophersecurity practices of their suppliers and service providers, including their secure development procedures. Permiter States shall also ensure that, when considering which measures referred to in that point are appropriate, entries are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).	Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (ii), of this Article are appropriate, entitles take into account the vulnerabilities specific to sech direct supplier and service provider and the overall quality of products and opherecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entries are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with article 2711.	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 miligating actions and monitoring performance against those plans.	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (ii), of this Article are appropriate, entitles take into account the vulnerabilities specific to sech direct supplier and service provider and the overall quality of products and ophersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entries are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with article 2711.	Functional	intersects with	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailoned development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (ii), of this Article are appropriate, entitles take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and operaccurity practices of their suppliers and service providers, including their secure development procedures. Permiser States shall also ensure that, when considering which measures referred to in that point are appropriate, entries are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 2211.	Functional	intersects with	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are paperprise, entitles take into account the vulnerabilities specific to sech direct supplier and service provider and the overall quality of products and opherecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entries are required to take into account the results of the coordinated security risk sessesments of critical supply chains carried out in accordance with Article 2211.	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entitles take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and ojbersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entries are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).	Functional	intersects with	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Senvice Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, poil (d), of this Article are paperpriste, entitles take into account the vulnerabilities specific to d), of this Article are paperpristed. The provider and the overall quality of products and ophersecurity practices of their supplier and service providers, including their secure development procedures. Hember States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments or critical supply character carried out in accordance with	Functional	intersects with	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
Article 21.3	N/A	Article 22711.  Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are apportine, entitles take into account the vulnerabilities specific to each firest supplier and service provider and the overall quality of products and ophersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with	Functional	intersects with	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.	5	
Article 21.3	N/A	Article 22711.  Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entitles take into account the vulnerabilities specific to each firest supplier and service provider and the overall quality of products and presence of their suppliers and service providers in the overall providers and the overall quality of products and operance of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with	Functional	intersects with	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique systems, system components or services.	5	
Article 21.3	N/A	Article 22711.  Member States shall ensure that, when considering which measures referred to in baragash 2, point (d), of this Article are apportine, entitles take into account the vulnerabilities specific to each first supplier and service provider and the overall quality of products and ophersecurity practices of their suppliers and service providers, including their secure development procedures. Hember States shall also ensure that, when considering which measures referred to in that point are appropriate, entries are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 2271.	Functional	intersects with	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	5	
Article 21.3	N/A	Andre 2011.  **Member States shall ensure that, when considering which measures referred to in paragash 2, point (d), of this Article are apportine, entities take into account the vulnerabilities people to each first supplier and service provider and the overall quality of products and operacurity practices of their suppliers and service providers, including their secure development procedures. Permiser States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 2211.	Functional	intersects with	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	5	
Article 21.3	N/A	Affects (221).  Affects (221).  Any and (221).  A point (a), of this Article are appropriate, entities take into account the jura graph 2, point (a), of this Article are appropriate, entities take into account the valuer adulties appendit to each direct supplier and service provider and the overall quality of products and opened preservably aractices of their suppliers and service years of the providers, including their secure development procedures. Preferred States shall also ensure that, when considering which measures referred to in the part and appropriate, entities are required to also into account the results of the coordinated successify risk assessments of critical supply chains carried out in accordance with Arelas 2731.	Functional	intersects with	Third-Party Services	TPM-04	Mechaniams exist to mitigate the risks associated with third-party access to the organization's systems and data.	5	



FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		Member States shall ensure that, when considering which measures referred to in					Mechanisms exist to conduct a risk assessment prior to the acquisition or	(optional)	
Article 21.3	N/A	paragraph 2, point (d), of this Article are appropriate, entitles take into account the vulnerabilities peoficit to each direct explaine and service provider and the overall quality of products and optersecurity practices of their suppliers and service providers, including their secure development procedures. Perhember States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 2271.	Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	outsourcing of technology-related services.	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (ii), of this Article are appropriate, entitles take into account the values of the state of the certain quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 2711.	Functional	intersects with	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (§), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and oper-security practices of their suppliers and service providers, including their secure development procedures. Perhapier States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 2711.	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 ta systems, processes and data.	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (ii), of this Article are appropriate, entities take into account the watershillites specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 2211.	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.	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (ii), of this Article are appropriate, entitles take into account the valnerabilities specific to each direct supplier and service provider and the overall quality of products and opersecurity practices of their suppliers and service providers, including their secure development procedures. Perhember States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 2211.	Functional	intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Censulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cyclersocurity & data privacy controls between internal stakeholders and External Service Providers (ESPs).	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (6), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and operaceunity practices of their suppliers and service providers, including their secure devolopment procedures. Pember States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 2711.	Functional	intersects with	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supporthe, Consulted & Informet (RASCI) match, or similar documentation, to ensure cybersecurity & data privacy control assignments occur	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (§), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and oper-security practices of their suppliers and service providers, including their secure development procedures. Permiser States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 2711.	Functional	intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (TPD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cyleraccurity & data privacy controls, including any flow-down requirements to subcontractors.	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures retired to in paragraph 2, point (§), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and operaceunity practices of their suppliers and service providers, including their secure devolopment procedures. Pember States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 2711.	Functional	intersects with	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersacurity and/or data privacy controls.	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragrand 2, point (ii), of this Article are papproprise, entitles take into account the vulnerabilities specific to each direct supplier and service provider and the overall qualify of products and operaceurity practices of their suppliers and service providers, including their secure development procedures. Pember States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk sasessments of critical supply chains carried out in accordance with Article 2211.	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.	5	
Article 21.3	N/A	Name of the state shall ensure that, when considering which measures referred to in paragraph 2, point (q), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and operaceunity practices of their suppliers and service providers, including their secure devolopment procedures. Permiser States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 2711.	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	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (ii), of this Article are appropriate, entities take into account the valurabilities specific to each direct supplier and service provider and the overall quality of products and ophersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 2211.	Functional	intersects with	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (ii), of this Article are appropriate, entitles take into account the values of the products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 2711.	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.	5	
Article 21.4	N/A	Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.	Functional	intersects with	Non-Compliance Oversight	CPL-01.1	Mechanisms exist to document and review instances of non-compliance with statutory, regulatory and/or contractual obligations to develop appropriate risk mitigation actions.	5	
Article 21.4	N/A	Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.	Functional	intersects with	Threat Analysis & Flaw Remediation During Development	IAO-04	Mechanisms exist to require system developers and integrators to create and execute a Security Testing and Evaluation (ST&E) plan, or similar process, to identify and remediate flaws during development.	5	
Article 21.4	N/A	Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.	Functional	intersects with	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.	5	
Article 21.4	N/A	Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
Article 21.4	N/A	Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.	Functional	intersects with	Developer Threat Analysis & Flaw Remediation	TDA-15	Mechanisms exist to require system developers and integrators to develop and implement an ongoing Security Testing and Evaluation (ST&E) plan, or similar process, to objectively identify and remediate vulnerabilities prior to release to production.	5	
Article 21.4	N/A	Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.	Functional	intersects with	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
Article 21.4	N/A	Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.	Functional	intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
Article 21.4	N/A	Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.	Functional	intersects with	Continuous Vulnerability Remediation Activities	VPM-04	Mechanisms exist to address new threats and vulnerabilities on an ongoing basis and ensure assets are protected against known attacks.	5	
Article 21.4	N/A	Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.	Functional	intersects with	Centralized Management of Flaw Remediation Processes	VPM-05.1	Mechanisms exist to centrally-manage the flaw remediation process.	5	



FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		By 17 October 2024, the Commission shall adopt implementing acts laying down the					Mechanisms exist to develop, document and maintain secure baseline	(optional)	
Article 21.5	N/A	technical and the methodological requirements of the measures referred to in paragan? 2 with regard to DNS service providers. I.D mane registries, cloud computing service providers, data entire service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
Article 21.5	N/A	by 17 october 2024, the Commission shall adopt implementing acts bying down the scholical and the methodological requirements of the measures referred to in paragraph 2 with regard to DNS service providers, LD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of ceiline search engines and of social networking services patternms, and trust service providers.	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).	5	
Article 21.5	N/A	By 17 October 2024, the Commission shall adopt implementing acts laying down the technical and the methodological requirements of the measures referred to in paragraph? With regard to DNS service providers, 11D name registries, close comparing service providers, 6 take centre registries, content delivery retworks rowiders, managed security service providers, managed security service providers, providers of online market places, of celline search engines and of social networking services platforms, and trust service providers.	Functional	subset of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized optersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
Article 23.1	NA	Each Member State shall ensure that essential and important entities notify, without undue delay its CSIT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 5 (significant incident). Where appropriate short expenses are services or effective to in paragraph 5 (significant incident). Where appropriate short short soft provision of those services of significant incidents that are likely to aversely affect the provision of those services. Each Member State shall ensure that those entities report, inter alia, any information anabiling the CSIT or, where applicable, the competent anotherly to determine yor cross-border impact of the incident. The mere act of notification shall not subject the notifying entity to increased liability.  Where the entities concerned notify the competent authority of a significant incident under the first subparagraph, the Member State shall ensure that that competent authority foverests the notification to the CSIRT upon receipt.  In the case of a cross-border or cross-sectors significant incident, Member States	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	
		shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with paragraph 4.							
Article 23.1	NA	Each Member State shall ensure that easential and important entities notify, without undue tellay, its CSRT or, where applicable, its competent authority in accordance with passing and 4 only inclicent that has a significant impact on the provision of the feet with passing and 4 only inclicent that has a significant inclicent on the provision of these concerned shall notify, without undue delay, the recipients of their services of significant inclines that are likely to adversely affect the provision of those services. Each Member State shall ensure that those entities report, inter alia, any information anabiling the CSRT or, where applicable, the competent authority to determine sory cross-border impact of the incident. The mere act of notification shall not subject the notifying entity to increased liability.  Where the entities concerned notify the competent authority of a significant incident.	Functional	intersects with	Incident Handling	IRO-02	Mechaniams exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
		under the first subgaragesph, the Member State shall ensure that that competent submöring forewise the notification to the CSRT upon receipt.  In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with puragesph 4.							
Article 23.1	N/A	Each Member State shall ensure that essential and important entities notify, without funde delay, its CSIT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph (significant incident), where appropriate, entitles concerned shall notify, without undue delay, the recipients of their services of regarders that are likely to absence yield. The provision of those services. Each Member State shall ensure that those entities report, ther alia, any information modeling the CSIT or, where applicable, the competent authority to determine any considerable of their control or their services. The meet act of notification shall not subject the notifying entity to increased liability.  Where the entities concerned notify the competent authority of a significant incident under the first suboparagraph, the Member State shall ensure that that competent	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (() Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
		authority forwards the notification to the CSRRT upon receipt.  In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with prangraph 4.							
Article 23.2	N/A	Where applicable, Member States shall ensure that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entitles shall also inform those recipients of the significant cyber threat itself.	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	
Article 23.2	N/A	Where applicable, Member States shall ensure that essential and important entities communicate, without unde delay, to the recipients of their services that are potentially affected by a significant ordjet threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entitles shall also inform those recipients of the significant cryber threat itself.	Functional	intersects with	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity & data privacy incident information to the provider of the product or service and bethe organizations moleved in the supply chain for systems or system components related to the incident.	5	
Article 23.2	N/A	Where applicable, Member States shall ensure that essential and important entities communicate, without unde delay, to the recipients of their achies that are potentially affected by a significant origin their surpressure or remedies that those recipients are able to take in response to that threat. Where appointed, the entitles shall also inform those recipients of the significant cyber threat itself.	Functional	intersects with	Public Relations & Reputation Repair	IRO-16	Mechanisms exist to proactively manage public relations associated with incidents and employ appropriate measures to prevent further reputational damage and develop plans to repair any damage to the organization's reputation.	5	
Article 23.3	N/A	An incident shall be considered to be significant if:	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	
Article 23.3(a)	N/A	It has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;	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	
Article 23.3(b)	N/A	it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.	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	
Article 23.4	N/A	Member Sates shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority.  By way of derogation from the first subparagraph, point (b), a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notly the CSIRT or, where applicable, the competent submit only without under delay and in any event within 25 hours or the comignious ware of the significant control of the competent submit only without under delay and in any event within 25 hours or the comignious ware of the significant control of the competent submit of the competen	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-eport incidents to applicable: (() Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
Article 23.4(a)	N/A	Incident.  without undue delay and in any event within 24 hours of becoming sware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;	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	
Article 23.4(b)	N/A	without undue delay and in any event within 27 hours of becoming aware of the significant inclider, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise:	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	
Article 23.4(c)	N/A	upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates;	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. Mechanisms exist to timely-report incidents to applicable:	5	
Article 23.4(d)	N/A	a final report not later than one month after the submission of the incident notification under point (b), including the following:	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	(1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities. Mechanisms exist to timely-report incidents to applicable:	5	
Article 23.4(d)(i)	N/A	a detailed description of the incident, including its severity and impact;	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	(1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities. Mechanisms exist to timely-report incidents to applicable:	5	
Article 23.4(d)(ii)	N/A	the type of threat or root cause that is likely to have triggered the incident;	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	(1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	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)
Article 23.4(d)(ii)	N/A	the type of threat or root cause that is likely to have triggered the incident;	Functional	equal	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	
Article 23.4(d)(iii)	N/A	applied and ongoing mitigation measures;	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	
Article 23.4(d)(iv)	N/A	where applicable, the cross-border impact of the incident;	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
Article 23.4(e)	N/A	in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
Article 23.5	N/A	The CSRT or the competent authority shall provide, without undue delay and where possible within 24 hours of receiving the early warring referred to in prangraph 4, point (a), a response to the notifying entity, louisding initial redeals do in the significant incident and, upon request of the entity, guidance or operational advice on the implementation of possible mitigation measures. Where the CSRT is not the initial receipent of the notification referred to in paragraph 1, the guidance shall be provided by the competent authority in cooperation with the CSRT. The CSRT shall provide additional technical support if the entity concerned so requests. Where the significant incident is suspected to be of criminal nature, the CSRT or the competent authority shall also provide guidance on reporting the significant incident to law enforcement authority.	Functional	no relationship	N/A	N/A	N/A	N/A	Outside of the scope of the SCF
Article 23.6	N/A	Where appropriate, also, it is particular volves the significant incident injoin commands to when the appropriate, also, it is particular volves the significant incident injoin contact shall inform, without undux delay, the other affected Member States and ENSA of the significant incident. Such information received in accordance with sparagraph. 4. In so doing, the CSIRT, the competent authority or the single point of contact shall, in accordance with thiolon or insteal law, preserve the entity's security and commencial interests as well as the confidentiality of the information provided in the confidentiality of the information providentiality of the information provided in the confidentiality of the information providentiality of the information providentiali	Functional	no relationship	N/A	N/A	N/A	N/A	Outside of the scope of the SCF
Article 23.7	N/A	Where public awareness is necessary to prevent a significant incident or to deal with an orgoing significant incident, or where disclosure of the significant incident is otherwise in the public interest, a Hembe State's CSRT's, where applicable, its competent authority, and, where appropriate, the CSRT's or the competent authorities of other Member States concerned, may, after consulting the ently concerned, inform the public about the significant incident or require the entity to do so.	Functional	no relationship	N/A	N/A	N/A	N/A	Outside of the scope of the SCF
Article 23.8	N/A	At the request of the CSIRT or the competent authority, the single point of contact shall forward notifications received pursuant to paragraph 1 to the single points of contact of other affected Member States.	Functional	no relationship	N/A	N/A	N/A	N/A	Outside of the scope of the SCF
Article 23.9	N/A	The single point of contact shall submit to ENSK every firste months a summary report, including anonymised and aggregated data on significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 3th in order to contribute to the provision of comparable information ENSK may adopt technical guidance on the parameters of the information to be included in the summary report. ENSK shall inform the Cooperation Group and the circle of the contribute of the contrib	Functional	no relationship	N/A	N/A	N/A	N/A	Outside of the scope of the SCF
Article 23.10	N/A	The CSIRTs or, where applicable, the competent authorities shall provide to the competent authorities under Directive (EU) 2022/2557 information about significant incidents, incidents, cyber threats and near misses notified in accordance with paragraph 1 of this Article and with Article 30 by entities identified as critical entities under Directive EUI 2022/2557.	Functional	no relationship	N/A	N/A	N/A	N/A	Outside of the scope of the SCF
Article 23.11	N/A	The Commission may adopt implementing acts further specifying the type of information, the format and the procedure of a notification submitted pursuant to paragraph 1 of this Article and to Article 3 and of a Commission submitted pursuant to paragraph 2 of this Article. All the Article 3 and of a Commission submitted pursuant to paragraph 2 of this Article. By 17 toctober 2014, the Commission shall, with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, active content delivery network providers, managed service providers, managed security service providers, as well as providers of online managed service providers, managed security service providers, as well as providers of online managed service providers, managed security servicing the cases in which an incident shall be considered to be significant as developing the cases in which an incident shall be considered to be significant to the reserved to prangraph 3. The Commission may adopt such implementing acts with regard to other essential and important entities.  The Commission shall exchange adobte and cooperate with the Cooperation Group on the draft implementing acts referred to in the first and second subparagraphs of this paragraph in accordance with Article 444, point (e.).  Those implementing acts afail to adopted in accordance with the examination procedure referred to in Article 20(2).	Functional	no relationship	N/A	N/A	N/A	N/A	Outside of the scope of the SCF

