NIST IR 847-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2025.3
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02022L2555-2022
have a first and a second of the second of t

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 under their operations or for the provision of their services, and to prevent or minimise the impact of includes no recipients of their services and not 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 shall an enternal as level of security of retwork 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 suppose to triaks, the entity's size and the illustroad of occurrence of Incidents and their seventy, including their accelett 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 or their operations or for the provision of their services, and to prevent or minimise the impact of includes no recipients of their services, and not her 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 an enternal service and on other developmentation systems appropriate to the risks posed. When assessing the proportionally of those measures, the activity's size and the likelihood of occurrence of incidents and their seventy, including their societat 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 cybersecurity and 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 entities or their operations or for the provision of their services, and to prevent or minimise the impact of includes no recipients of their services, and not her services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of level feedings to the restrict of the cost of their operations of the restrict of the cost of their operations of the restrict on the first subgraga pin shall ensure a level of security of reversive and international standards, as well as the cost of level free restrict on the restrict of the rest	Functional	intersects with	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review Technology Assets, Applications and/or Services (TAAS) and American to the organization's cybersecurity and 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 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 includins on recipients of their services and not 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 subgragaph shall ensure a level of security of retwork 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 suppose to triaks, the entity's size and the likelihood of occurrence of incidents and their severity, including their accelet and accounts' impact.	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and 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 immation systems which those entities or their operations or for the provision of their services, and to prevent or minimise the impact of includins on recipients of their services, and not her services. The impact of the impact of the services and not her services and not her services. The impact of the services are services and not her services and international standards, as well as the cost of level impenentation, the measures referred to in the first subgraph shall ensure select of security retwork and information systems appropriate to the risks posed. When assessing the proportionality of those sensures, due and the illustroad of occurrence of Incidents and their severity, including their accelett and economic impact.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	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 to prevent or minimise the impact of incidents or recipients of their services and on other services. Taking important the state-of-the-ert and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subgrapages hall ensure a level of security of retextor 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 seposure to foreight the internity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechaniams exist to compet data and/or process owners to operationalize cyber security and data protection practices for each Technology Asset, Application and/or Service (TAKS) 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 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. Taking into account the state-of-the-erf 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 poach. When assessing the proportionality of the emeasures, due account shall be taken of the degree of the entity's sexposure to risks, the entity's size not the likelihood of occurrence of incidents and their severity, including their societal and economic impact.	Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compet data and/or process owners to select required cyber security and data protection controls for each Technology Asset, Application and/or Service (TAAS) 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 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 on other services and increase of their services and on other services and an attendance of their services and on other services or their services and on other services or their 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 poach. When assessing the proportionality of the offers subparagraph shall ensure a level of security of network and information systems appropriate to the risks poach. When assessing the proportionality of the entity's is another to the identity of courance or incidents and their severity, including their societal and economic impact.	Functional	intersects with	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required cyber security and data protection controls for each Technology Asset, Application and/or Service (TAAS) 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 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 to prevent or minimise the impact of incidents on recipients of their services and on other services. Taking into account the state-of-the-ert and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subgrapages hall ensure a level of security of retextor, and internationally of those measures, use count shall be taken of the degree of the entity's exposure to risk, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.	Functional	intersects with	Risk Management Program	RSK-01	Mechanisms 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	(optional)	
		Member States snau 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					likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's Technology Assets,		
		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.					Applications, Services and/or Data (TAASD).		
Article 21.1	N/A	Taking into account the state-of-the-art and, where applicable, relevant European and	Functional	intersects with	Risk Assessment	RSK-04		5	
		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 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 and data protection practices in the specification, design,		
		proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for					development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).		
		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	Functional	intersects with	Secure Engineering Principles	SEA-01		5	
		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 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 and 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 and data		
Article 21.2(a)	N/A	policies on risk analysis and information system security;	Functional	subset of	Protection Governance Program	GOV-01	protection governance controls.	10	
Article 21.2(a)	N/A	policies on risk analysis and information system security;	Functional	intersects with	Publishing Cybersecurity & Data Protection	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	
		, , , , , , , , , , , , , , , , , , , ,			Documentation		Menhaniama aviet to compal descriptions	-	
Article 21.2(a)	N/A	policies on risk analysis and information system security;	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compet data and/or process owners to operationalize cybersecurity and data protection practices for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
Article 21.2(a)	N/A	policies on risk analysis and information system security;	Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity and data protection controls for each Technology Asset, Application	5	
							and/or Service (TAAS) under their control. Mechanisms exist to compel data and/or process owners to implement required		
Article 21.2(a)	N/A	policies on risk analysis and information system security;	Functional	intersects with	Implement Controls Risk Management	GOV-15.2	cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) 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	Program Cybersecurity & Data	RSK-01	recreamsms exist to facilitate the implementation of strategic, operational and tactical risk management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data	5	
Article 21.2(b)	N/A	incident handling;	Functional	subset of	Protection Governance Program	GOV-01	protection governance controls.	10	
Article 21.2(b)	N/A	incident handling;	Functional	intersects with	Publishing Cybersecurity & Data Protection	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	
					Documentation Operationalizing		Mechanisms exist to compel data and/or process owners to operationalize		
Article 21.2(b)	N/A	incident handling;	Functional	intersects with	Cybersecurity & Data Protection Practices	GOV-15	rectinations exist to complete that animon process owners to operationalize cybersecurity and data protection practices for each Technology Asset, Application and/or Service (TAAS) under their control.	5	
Article 21.2(b)	N/A	incident handling;	Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity and data protection controls for each Technology Asset, Application	5	
							and/or Service (TAAS) under their control. Mechanisms exist to compel data and/or process owners to implement required	5	
Article 21.2(b)	N/A	incident handling;	Functional	intersects with	Implement Controls	GOV-15.2	cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) under their control. Mechanisms exist to implement and govern processes and documentation to	ь	
Article 21.2(b)	N/A	incident handling;	Functional	intersects with	Incident Response Operations	IRO-01	facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
							Mechanisms exist to cover: (1) Preparation;		
Article 21.2(b)	N/A	incident handling:	Functional	intersects with	Incident Handling	IRO-02	(2) Automated event detection or manual incident report intake; (3) Analysis;	5	
							(4) Containment; (5) Eradication; and (6) Recovery		
Article 21.2(c)	N/A	business continuity, such as backup management and disaster recovery, and crisis	Functional	subset of	Business Continuity Management System	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g.,	10	
At ticle 21.2(c)	IVA	management;	runctional	subset of	(BCMS)	BCD-01	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 management;	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	
		-			Information System		the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). Mechanisms exist to ensure the secure recovery and reconstitution of Technology		
Article 21.2(c)	N/A	business continuity, such as backup management and disaster recovery, and crisis management;	Functional	intersects with	Recovery & Reconstitution	BCD-12	Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
Article 21.2(c)	N/A	business continuity, such as backup management and disaster recovery, and crisis management;	Functional	subset of	Cybersecurity & Data Protection Governance	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
		business continuity, such as backup management and disaster recovery, and crisis			Program Publishing Cybersecurity		Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.		
Article 21.2(c)	N/A	management;	Functional	intersects with	& Data Protection Documentation	GOV-02		5	
Article 21.2(c)	N/A	business continuity, such as backup management and disaster recovery, and crisis management;	Functional	intersects with	Operationalizing Cybersecurity & Data	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each Technology Asset, Application	5	
Article 21.2(c)	N/A	business continuity, such as backup management and disaster recovery, and crisis	Functional	intersects with	Protection Practices Select Controls	GOV-15.1	and/or Service (TAAS) under their control. Mechanisms exist to compel data and/or process owners to select required cybersecurity and data protection controls for each Technology Asset, Application	5	
		management;					and/or Service (TAAS) under their control. Mechanisms exist to compel data and/or process owners to implement required		
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 and data protection controls for each Technology Asset, Application and/or Service (TAAS) 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	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
		supply chain security, including security-related aspects concerning the relationships	F	total and a single	Publishing Cybersecurity	00	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	_	
Article 21.2(d)	N/A	between each entity and its direct suppliers or service providers;	Functional	intersects with	& Data Protection Documentation	GOV-02		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	Operationalizing Cybersecurity & Data	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each Technology Asset, Application	5	
Article 21.2(d)	N/A	supply chain security, including security-related aspects concerning the relationships	Functional	intersects with	Protection Practices Select Controls	GOV-15 1	and/or Service (TAAS) under their control. Mechanisms exist to compel data and/or process owners to select required cybersecurity and data protection controls for each Technology Asset, Application	5	
		between each entity and its direct suppliers or service providers;					and/or Service (TAAS) under their control. Mechanisms exist to compel data and/or process owners to implement required	-	
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	GOV-15.2	cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) 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	Functional	intersects with	Supply Chain Risk	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of Technology Assets, Applications and/or Services (TAAS), including documenting	5	
		between each entity and its direct suppliers or service providers;			Management (SCRM) Plan	00	selected mitigating actions and monitoring performance against those plans.		
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	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
Article 21.2(d)	N/A	supply chain security, including security-related aspects concerning the relationships	Functional	intersects with	Supply Chain Risk	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Sandons (TAAS) supply chains; and	5	
~ dute 21.2(0)	IVA	between each entity and its direct suppliers or service providers;	, uncoonst	secus with	Management (SCRM)	1-1-03	Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.		
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	Mechanisms suit turious, as recessary, Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
<u> </u>		, moveing removement manading and discussing,		1	Program			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(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 Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	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 and data protection practices for each Technology Asset, Application	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	and/or Service (TAAS) under their control. Mechanisms exist to compel data and/or process owners to select required cybersecurity and data protection controls for each Technology Asset, Application	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	GOV-15.2	and/or Service (TAAS) under their control. Mechanisms exist to compel data and/or process owners to implement required	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	cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) 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	Functional	intersects with	Network Security	NET-01	the implementation of maintenance controls across the enterprise. Mechanisms exist to develop, govern & update procedures to facilitate the	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	Technology Development	TDA-01	implementation of Network Security Controls (NSC). Mechanisms exist to facilitate the implementation of tailored development and sequisition strategies, contract tools and procurement methods to meet unique	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	& Acquisition Third-Party Management	TPM-01	business needs. Mechanisms exist to facilitate the implementation of third-party management	5	
Article 21.2(e)	N/A	maintenance, including vulnerabulity handling and disclosure; security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	Functional	intersects with	Vulnerability & Patch Management Program	VPM-01	controls. Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
Article 21.2ff)	N/A	policies and procedures to assess the effectiveness of cybersecurity risk-	Functional	subset of	(VPMP) Cybersecurity & Data Protection Governance	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
		management measures;			Program		Mechanisms exist to coordinate cybersecurity, data protection and business	-	
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	slignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis. Mechanisms exist to establish, maintain and disseminate cybersecurity and data	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	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 and data protection 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 and data protection practices for each Technology Asset, Application and/or Service (TAAS) 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 compet data and/or process owners to select required cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) 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 and data protection controls for each Technology Asset, Application and/or Service (TAAS) 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	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
Article 21.2(g)	N/A	basic cyber hygiene practices and cybersecurity training;	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
Article 21.2(g)	N/A	basic cyber hygiene practices and cybersecurity training:	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	
Article 21.2(g)	N/A	basic cyber hygiene practices and cybersecurity training;	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each Technology Asset, Application and/or Service (TAAS) 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 compel data and/or process owners to select required cybersecurity and data protection controls for each Technology Asset, Application	5	
Article 21.2(g)	N/A	basic cyber hygiene practices and cybersecurity training;	Functional	intersects with	Implement Controls	GOV-15.2	and/or Service (TAAS) under their control. Mechanisms exist to compel data and/or process owners to implement required cybersecurity and data protection controls for each Technology Asset, Application	5	
Article 21.2(g)	N/A	basic cyber hygiene practices and cybersecurity training;	Functional	intersects with	Cybersecurity & Data Protection-Minded	SAT-01	and/or Service (TAAS) under their control. 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	Workforce 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,	Functional	subset of	Cybersecurity & Data Protection Governance	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection governance controls.	10	
Article 21.2(h)	N/A	encryption; policies and procedures regarding the use of cryptography and, where appropriate, encryption;	Functional	intersects with	Program Publishing Cybersecurity & Data Protection	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	5	
Article 21.2(h)	N/A	policies and procedures regarding the use of cryptography and, where appropriate,	Functional	intersects with	Operationalizing Cybersecurity & Data	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each Technology Asset, Application	5	
Article 21.2(h)	N/A	encryption; policies and procedures regarding the use of cryptography and, where appropriate,	Functional	intersects with	Protection Practices Select Controls	GOV-15.1	and/or Service (TAAS) under their control. Mechanisms exist to compel data and/or process owners to select required cybersecurity and data protection controls for each Technology Asset, Application	5	
		encryption; policies and procedures regarding the use of cryptography and, where appropriate,		intersects with			and/or Service (TAAS) under their control. Mechanisms exist to compel data and/or process owners to implement required	_	
Article 21.2(h) Article 21.2(i)	N/A N/A	encryption; human resources security, access control policies and asset management;	Functional	intersects with	Implement Controls Asset Governance	GOV-15.2 AST-01	cybersecurity and data protection controls for each Technology Asset, Application and/or Service (TAAS) under their control. Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement	5	
Article 21.2(I)	N/A	numan resources security, access control policies and asset management;	Functional	intersects with	Asset Governance	AS1-01	and manage asset management controls. Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/Or Data (TAASD) that:		
							(1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details;		
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	
							(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 and data protection governance controls.	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 and 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 and data protection practices for each Technology Asset, Application and/or Service (TAAS) 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 and data protection controls for each Technology Asset, Application and/or Service (TAAS) 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 and data protection controls for each Technology Asset, Application and/or Service (TAAS) 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	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	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	Identity & Access Management (IAM) Cybersecurity & Data	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls. Mechanisms exist to facilitate the implementation of cybersecurity and data	5	
Article 21.2(j)	N/A	vice, video and text communications and secured emergency communication systems within the entity, where appropriate.	Functional	subset of	Protection Governance Program	GOV-01	protection governance controls.	10	
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	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data 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 engroyide.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity and data protection practices for each Technology Asset, Application	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	Protection Practices Select Controls	GOV-15.1	and/or Service (TAAS) under their control. Mechanisms exist to compel data and/or process owners to select required cybersecurity and data protection controls for each Technology Asset, Application	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	Implement Controls		and/or Service (TAAS) under their control. Mechanisms exist to compel data and/or process owners to implement required cybersecurity and data protection controls for each Technology Asset, Application	5	
-		systems within the entity, where appropriate. the use of multi-factor authentication or continuous authentication solutions, secured			Identity & Access		and/or Service (TAAS) under their control. Mechanisms exist to facilitate the implementation of identification and access		
Article 21.2(j)	N/A	voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	Functional	intersects with	Management (IAM)	IAC-01	management controls.	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)
			Rationale	Retationship			Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:	(optional)	
Article 21.2(j)	N/A	the use of multi-factor suthentication 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	(1) Remote network access; Q2 Third-party Fechnology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures reterred to in parragraph 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 operacurity practices of their suppliers and service providers, including their secure development procedures. Perhapter 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 Protection in Project Management	PRM-04	Mechanisms exist to assess cybersecurity and data protection 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 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 ophersecurity practices of their suppliers and service providers, including their secure development procedures. Perfember 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	Cybersecurity & Data Protection Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a critically analysis for critical Technology Assets, Applications and/or Services (TAAS) at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
Article 21.3	N/A	Hember States shall ensure that, when considering which measures referred to in paragraph 2, point (ii), of the Article are appropriate, entitles take into account the vulnerabilities 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. 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 sessesments of critical supply chains carried out in accordance with Article 2711.	Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TASA) 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 each direct supplier and service provider and the overst! 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, 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	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Hanagement (SCRM) associated with the development, capulation, maintenance and disposal of Technology Assets, Applications and/or/Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
Article 21.3	N/A	Hember 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 understabilities specific to each direct supplier and service provider and the overstill 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 2211.	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, entities take into account the vulnerabilities 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 sessesments 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	Hember 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 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, 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 2711.	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 retirent 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 operaceurity practices of their suppliers and service providers, including their secure development procedures. Perfember States shall also ensure that, when considering which measures reterred 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	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and ord Safety (CIAIS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures reterred to in parragraph 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 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	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) 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	Member States shall ensure that, when considering which measures reterred to in orange not, 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 open-security practices of their suppliers and service providers, including their secure development procedures. Perfember States shall also ensure that, when considering which measures reterred 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	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
Article 21.3	N/A	Notice 2 is a service of the considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the valuerabilities people to each firest supplier and service provider and the overall quality of products and operacurity practices of their suppliers and service providers, including their secure development procedures. Perhapse 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 sessesments of critical supply chains carried out in accordance with Article 2711.	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 Technology Assets, Applications and/or Services (TAAS).	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 oper-security practices of their suppliers and service providers, including their secure development procedures. Perfember 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	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	Hember 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 understabilities specific to each direct supplier and service provider and the overstill 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 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	Member States shall ensure that, when considering which measures referred to in paragraph 2, porting, of this Article are appropriate, entitles take into account the values of the paragraph 2 of the pa	Functional	intersects with	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	

EU NIS2 Directive



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 Junkmenblitise specific to each direct explicit and service provides and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Hermber 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 Technology Assets, Applications and/or Services (TAAS).	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 value of the state of the state of the state of the state of the count of the value of the state of the 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 retired 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 opersecurity practices of their suppliers and service providers, including their secure development procedures. Perfember States shall also ensure that, when considering which measures reterred 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 and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	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 watershallities 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, artisties 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	Machanisms exist to ensure cybersecurity and data protection 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 (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 opersecurity practices of their suppliers and service providers, including their secure development procedures. Perfember 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, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cyber security and data protection 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 (g), 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 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 2711.	Functional	intersects with	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supporhe, Consulted & Informed (RASC) matrix, or similar documentation, to ensure ophersecurity and data protection control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (g), 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 operaceurity 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, artistics 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 (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity and data protection controls, including any flow-down requirements to subcontractors.	5	
Article 21.3	N/A	Member States shall ensure that, when considering which measures referred to in paragraph 2, point (g), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overail quality of products and operaceunity practices of their suppliers and service providers, including their secure development procedures. Perhapse States shall also ensure that, when considering which measures referred to in that point are appropriate, antities 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 cybersecurity and/or 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 vulnerabilities specific to each direct supplier and service provider and the overall quality of products and operaceurity practices of their suppliers and service providers, including their secure development procedures. Perfember 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	Member States shall ensure that when considering which measures referred to in paragraph 2, point bits Article are appropriate, entities count the vulnerabilities specific to the Article are supplier and service provider and the overall quality of producing and pole-security practices of their suppliers and service providers, including their secure development procedures. Hember States and the providers, including their secure development procedures. Hember States are large consume that, when considering with interpretable to the procedure of the procedure security risk assessments of criticial surple operations of the security risk assessments of criticial surple security risk assessments of security risk assessments security risk assessments security risk asses	Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESP8) for compliance with established contractual requirements for cybersecurity and data protection controls.	5	
Article 21.3	N/A	Article 22/11. 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 underabilities 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. 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 of critical supply chains carried out in accordance with Article 22/11.	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 (d), of this Article are appropriate, entitles take into account the values of the state of the certain quality of products and cybersecurity practice 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 Technology Assets, Applications, Services and/or Data (TAASD) that are in acope 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 configurations for Technology Assets, Applications and/or Services (TAAS) that are	(optional)	
Article 21.5	N/A	technical and the methodological requirements of the measures referred to in paragraph 2 with regard to DNS service providers, TLD 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 online search engines and of social networking services	Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	consistent with industry-accepted system hardening standards.	5	
		platforms, and trust service providers.							
		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 2 with regard to DNS service providers, TLD name registries, cloud			Network Security		Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).		
Article 21.5	N/A	computing service providers, data centre 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	Controls (NSC)	NET-01		5	
		By 17 October 2024, the Commission shall adopt implementing acts laying down the technical and the methodological requirements of the measures referred to in					Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design,		
Article 21.5	N/A	paragraph 2 with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of colline market places, of online search engines and of social networking services platforms, and rust service providers.	Functional	subset of	Secure Engineering Principles	SEA-01	development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
Article 23.1	N/A	Each Member State shall ensure that essential and important entities notify, without undue delay, its CSRT or, where applicable, its competent authority in accordance with paragraph of any incident that has a significant import on the provision of their services as referred to in paragraph 3 (significant incident). Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services or significant incidents that are likely to adversely affect the provision of those services. Each Member State shall ensure that those entities report, inter sila, any information enabling the CSRT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere act of notification shall not subject the notifying entity to increased tiability.	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
		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 forwards the notification to the CSIRT upon receipt. In the case of a cross-border or cross-sectoral significant incident, Member States							
		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 paragraph 4. Each Member State shall ensure that essential and important entities notify, without					Mechanisms exist to cover:		
Article 23.1	N/A	can relative solate islate attained that exhibition is competent authority in accordance with paragon ph of any injustment that has a light interest authority in accordance with paragon ph of any injustment that has a significant incident. Where appropriate, entitled concerned what notify, whortun undue delay, the recipients of their avortice of registration of their avortice of significant incident, Where appropriate, entitled concerned what notify, whortun undue delay, the recipients of their avortice of significant incident, where appropriate, entitled concerned what notifies are reliable to accessed with a reliable to accessed with the provision of those services. Each Member State shall ensure that those entities report, inter alia, any information making the CSRT or, where appropriate provision is concerned without the control of the provision of the prov	Functional	intersects with	Incident Handling	IRO-02	(I) Preparation; 2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Enalication; and (6) Recovery.	5	
		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 forwards the notification to the CSIRT 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 paragraph 4.							
Article 23.1	N/A	Each Member State shall ensure that essential and important entities notify, without undue delay, its CSSIT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant indent on the provision of their services as referred to in paragraph (significant incident), where appropriate recipients of their services of resistence and shall notify, without undue delay, the recipients of their services of significant incidents that are likely to observe yiel entire provision of those services. Each Member State shall ensure that those entities report, inter alia, any information making the CSIT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere act of notification shall not subject the notifying entity to increased tilability. Where the entities concerned notly the competent authority of a significant 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	
		under the first subparagoph, the Nember State shall ensure that that competent suthority forwards the notification to the CSIRT upon receipt. In the case of a cross-border or cross-sectional significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with puragoph 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 tople threat any amesures 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	Mechanisma 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 entitles communicate, without undue delay, to the recipients of their services that are potentially affector by a significant cylor threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cycle threat itself.	Functional	intersects with	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide optersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TASA) and other organizations involved in the supply chain for TASS related to the incident.	5	
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 tople threat any amesures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities 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; it has affected or is capable of affecting other natural or legal persons by causing	Functional	intersects with	Incident Classification & Prioritization Incident Classification &	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions. Mechanisms exist to identify classes of incidents and actions to take to ensure the	5	
Article 23.3(b)	N/A	It may arrive the unit of papers or anieuting other hautard or legal persons by classing considerable material or non-material damage. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority:	Functional	intersects with	Prioritization	IRO-02.4	continuation of organizational missions and business functions. Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders;	5	
Article 23.4	N/A	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, notify the CSRT or, where applicable, the competent authority, without undue delay and in any event within 24 hours of becoming aware of the significant	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	(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 aware 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 (1) Benuldaru, suthorities	5	
Article 23.4(b)	N/A	without undue delay and in any event within 72 hours of becoming aware of the significant incident, 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	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	(3) Regulatory authorities. 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	of compromise: 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 (1) Beaulaton, exthorities	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	(3) Regulator suthorities. 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)(i)	N/A	a detailed description of the incident, including its severity and 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(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	Mechanisms exist to timely-report incidents to applicable: (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	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 and data protection incidents to reduce the likelihood or impact of future incidents.	(optional)	
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	NA	The CSIRT or the competent suthority shall provide, without undue delay and where possible within 24 hours of receiving the early warning referred to in paragraph A point (a), a response to the notifying entity, including initial redeals con the significant incident and, upon request of the entity, guidance or operational solvice on the implementation of possible mitigation measures. Where the CSIRT is not the initial recipient of the notification referred to in paragraph 1, the guidance shall be provided additional technical support if the entity concerned so requests. Where the significant incident is suspected to be of criminal nature, the CSIRT 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, and in particular where the significant incident concerns two or more Member States, the CSRT, the competent authority or the single point of contact shall inform, without undue delay, the other affected Member States and FNSA of the significant incident. Such information shall include the peye information received in accordance with paragraph. I in so doing, the CSRT, the competent authority or the single point of contact shall, in accordance with Union or noticeal law, preserve the entity's security and commercial interests as well as the confidentiality of the information provides.	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 organia significant incident, or where disclosure of the significant incident is otherwise in the public interest, a theme State's CSIRT, where applicable, its competent authority, and, where appropriate, the CSIRTs or the competent authorities of other Member States concerned, may, after consulting the entity concerned, inform the public about he 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 ENSA every three months a summary report, including anonymised and aggregated data on significant incidents, incidents, cyber threats and near misseen notified in accordance with paragraph 1 of this Article and with Article 3D. In order to contribute to the provision of comparable information ENSA may adopt technical guidance on the parameters of the information to be included in the summary report. ENSA shall inform the Cooperation Group and the circumstance of the contribution of the contributio	Functional	no relationship	N/A	N/A	NA	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 lincidents, 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 (EU) 2022/2557.	Functional	no relationship	N/A	N/A	N/A	N/A	Outside of the scope of the SCF
Article 23.11	NA	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 communication submitted pursuant to paragraph 2 of this Article. 3 for the Commission shall, with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, and content delayers prevent 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 service providers, as well as providers of online managed service providers, managed security services, managed service providers, managed security services, managed service providers, managed security services, managed services providers, managed security services, and the security of the security of the security services and security services and security services and security services and security services. The Commission shall exchange advices and cooperate with the Cooperation Group on the draft implementing acts referred to in the first and second subparagophin of this paragraph in accordance with Article 44(4), point (e). Those implementing acts and the adopted in accordance with the examination procedure referred to in Article 38(1).	Functional	no relationship	N/A	N/A	N/A	N/A	Outside of the scope of the SCF

