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

Focal Document: EU Cyber Resilience Act - Annexes
Focal Document URL: https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC_2&format=PDF
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-emea-eu-cyber-resilience-act-annexes.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Annex 1	Essential Cybersecurity Requirements	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 1.1	Security Requirements Relating To The Properties of Products With Digital Elements	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 1.1(1)	N/A	Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;	Functional	subset of	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce products and/or services in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	10	
Annex 1.1(2)	N/A	Products with digital elements shall be delivered without any known exploitable vulnerabilities;	Functional	equal	Minimizing Attack Surfaces	TDA-02.8	Mechanisms exist to minimize the attack surface of products and/or services by reasonably mitigating known exploitable vulnerabilities.	10	
Annex 1.1(3)	N/A	On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 1.1(3)(a)	N/A	be delivered with a secure by default configuration, including the possibility to reset the product to its original state;	Functional	subset of	Pre-Established Secure Configurations	TDA-02.4	Mechanisms exist to ensure vendors / manufacturers: (1) Deliver the system, component, or service with a pre-established, secure configuration implemented; and (2) Use the pre-established, secure configuration as the default for any subsequent system, component, or service reinstallation or upgrade.	10	
Annex 1.1(3)(b)	N/A	ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;	Functional	intersects with	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce products and/or services in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	8	
Annex 1.1(3)(c)	N/A	protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;	Functional	intersects with	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce products and/or services in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	8	
Annex 1.1(3)(d)	N/A	protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;	Functional	intersects with	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce products and/or services in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	8	
Annex 1.1(3)(e)	N/A	process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');	Functional	subset of	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	10	
Annex 1.1(3)(e)	N/A	process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');	Functional	intersects with	Defining Access Authorizations for Sensitive/Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data.	8	
Annex 1.1(3)(e)	N/A	process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');	Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	8	
Annex 1.1(3)(e)	N/A	process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');	Functional	intersects with	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	8	
Annex 1.1(3)(f)	N/A	protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;	Functional	intersects with	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce products and/or services in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	8	
Annex 1.1(3)(g)	N/A	minimise their own negative impact on the availability of services provided by other devices or networks;	Functional	intersects with	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce products and/or services in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	8	
Annex 1.1(3)(h)	N/A	be designed, developed and produced to limit attack surfaces, including external interfaces;	Functional	equal	Minimizing Attack Surfaces	TDA-02.8	Mechanisms exist to minimize the attack surface of products and/or services by reasonably mitigating known exploitable vulnerabilities.	10	
Annex 1.1(3)(i)	N/A	be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;	Functional	intersects with	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce products and/or services in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	8	
Annex 1.1(3)(j)	N/A	provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;	Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of products and/or services across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
Annex 1.1(3)(k)	N/A	ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users.	Functional	equal	Ongoing Product Security Support	TDA-02.9	Mechanisms exist to deliver security updates to products and/or services, where applicable, through: (1) Automatic updates; and (2) Notification of available updates to affected users.	10	
Annex 1.2	Vulnerability Handling Requirements	Manufacturers of the products with digital elements shall:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 1.2(1)	N/A	identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;	Functional	subset of	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for systems, applications and services that lists software packages in use, including versions and applicable licenses.	10	
Annex 1.2(2)	N/A	in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;	Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
Annex 1.2(2)	N/A	in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;	Functional	intersects with	Ongoing Product Security Support	TDA-02.9	Mechanisms exist to deliver security updates to Assets, Applications & Services (AAS), where applicable, through: (1) Automatic updates; and (2) Notification of available updates to affected users.	5	
Annex 1.2(3)	N/A	apply effective and regular tests and reviews of the security of the product with digital elements;	Functional	equal	Product Testing & Reviews	TDA-02.10	Mechanisms exist to regularly review Assets, Applications & Services (AAS) for an appropriate level of security and resiliency based on applicable risks and threats.	10	
Annex 1.2(4)	N/A	once a security update has been made available, publically disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities;	Functional	equal	Disclosure of Vulnerabilities	TDA-02.11	Mechanisms exist to disclose information about vulnerabilities to relevant stakeholders, including: (1) A description of the vulnerability(ies); (2) Affected product(s) and/or service(s); (3) Potential impact of the vulnerability(ies); (4) Severity of the vulnerability(ies); and (5) Guidance to remediate the vulnerability(ies).	10	
Annex 1.2(5)	N/A	put in place and enforce a policy on coordinated vulnerability disclosure;	Functional	subset of	Vulnerability Disclosure Program (VDP)	THR-06	Mechanisms exist to establish a Vulnerability Disclosure Program (VDP) to assist with the secure development and maintenance of Assets, Applications & Services (AAS) that receives unsolicited input from the public about vulnerabilities in organizational AAS.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Annex 1.2(6)	N/A	take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;	Functional	intersects with	Disclosure of Vulnerabilities	TDA-02.11	Mechanisms exist to disclose information about vulnerabilities to relevant stakeholders, including: (1) A description of the vulnerability(ies); (2) Affected product(s) and/or service(s); (3) Potential impact of the vulnerability(ies); (4) Severity of the vulnerability(ies); and (5) Guidance to remediate the vulnerability(ies).	8	
Annex 1.2(6)	N/A	take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;	Functional	subset of	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Assets, Applications & Services (AAS) that lists software packages in use, including versions and applicable licenses.	10	
Annex 1.2(7)	N/A	provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;	Functional	subset of	Ongoing Product Security Support	TDA-02.9	Mechanisms exist to deliver security updates to Assets, Applications & Services (AAS), where applicable, through: (1) Automatic updates; and (2) Notification of available updates to affected users.	10	
Annex 1.2(8)	N/A	ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.	Functional	intersects with	Ongoing Product Security Support	TDA-02.9	Mechanisms exist to deliver security updates to Assets, Applications & Services (AAS), where applicable, through: (1) Automatic updates; and (2) Notification of available updates to affected users.	5	
Annex 2	Information and Instructions To The User	As a minimum, the product with digital elements shall be accompanied by:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 2.1	N/A	the name, registered trade name or registered trade mark of the manufacturer, and the postal address and the email address at which the manufacturer can be contacted, on the product or, where that is not possible, on its packaging or in a document accompanying the product;	Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
Annex 2.2	N/A	the point of contact where information about cybersecurity vulnerabilities of the product can be reported and received;	Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
Annex 2.2	N/A	the point of contact where information about cybersecurity vulnerabilities of the product can be reported and received;	Functional	intersects with	Security Disclosure Contact Information	THR-06.1	Mechanisms exist to enable public submissions of discovered or potential security vulnerabilities.	5	
Annex 2.3	N/A	the correct identification of the type, batch, version or serial number or other element allowing the identification of the product and the corresponding instructions and user information;	Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
Annex 2.4	N/A	the intended use, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;	Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
Annex 2.5	N/A	any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;	Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
Annex 2.6	N/A	if and, where applicable, where the software bill of materials can be accessed;	Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
Annex 2.7	N/A	where applicable, the internet address at which the EU declaration of conformity can be accessed;	Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
Annex 2.8	N/A	the type of technical security support offered by the manufacturer and until when it will be provided, at the very least until when users can expect to receive security updates;	Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
Annex 2.9	N/A	detailed instructions or an internet address referring to such detailed instructions and information on:	Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
Annex 2.9(a)	N/A	the necessary measures during initial commissioning and throughout the lifetime of the product to ensure its secure use;	Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
Annex 2.9(b)	N/A	how changes to the product can affect the security of data;	Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Annex 2.9(c)	N/A	how security-relevant updates can be installed;	Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
Annex 2.9(d)	N/A	the secure decommissioning of the product, including information on how user data can be securely removed.	Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
Annex 3	Critical Products With Digital Elements	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 3 Class 1	N/A	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 3 Class 1.1	N/A	Identity management systems software and privileged access management software;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.2	N/A	Standalone and embedded browsers;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.3	N/A	Password managers;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.4	N/A	Software that searches for, removes, or quarantines malicious software;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.5	N/A	Products with digital elements with the function of virtual private network (VPN);	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.6	N/A	Network management systems;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.7	N/A	Network configuration management tools;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.8	N/A	Network traffic monitoring systems;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.9	N/A	Management of network resources;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.10	N/A	Security information and event management (SIEM) systems;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.11	N/A	Update/patch management, including boot managers;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.12	N/A	Application configuration management systems;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.13	N/A	Remote access/sharing software;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.14	N/A	Mobile device management software;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.15	N/A	Physical network interfaces;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.16	N/A	Operating systems not covered by class II;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.17	N/A	Firewalls, intrusion detection and/or prevention systems not covered by class II;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.18	N/A	Routers, modems intended for the connection to the internet, and switches, not covered by class II;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.19	N/A	Microprocessors not covered by class II;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.20	N/A	Microcontrollers;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.21	N/A	Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.22	N/A	Industrial Automation & Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 1.23	N/A	Industrial Internet of Things not covered by class II	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 2	N/A	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 3 Class 2.1	N/A	Operating systems for servers, desktops, and mobile devices;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 2.2	N/A	Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 2.3	N/A	Public key infrastructure and digital certificate issuers;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 2.4	N/A	Firewalls, intrusion detection and/or prevention systems intended for industrial use;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 2.5	N/A	General purpose microprocessors;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 2.6	N/A	Microprocessors intended for integration in programmable logic controllers and secure elements;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 2.7	N/A	Routers, modems intended for the connection to the internet, and switches, intended for industrial use;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 2.8	N/A	Secure elements;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 2.9	N/A	Hardware Security Modules (HSMs);	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 2.10	N/A	Secure cryptoprocessors;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 2.11	N/A	Smartcards, smartcard readers and tokens;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 2.12	N/A	Industrial Automation & Control Systems (IACS) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)], such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA);	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 2.13	N/A	Industrial Internet of Things devices intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)];	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 2.14	N/A	Robot sensing and actuator components and robot controllers;	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 3 Class 2.15	N/A	Smart meters.	Functional	subset of	Products With Digital Elements	TDA-02.12	Mechanisms exist to categorize applicable security and resiliency requirements for products and/or services with digital elements.	10	
Annex 4	EU Declaration of Conformity	The EU declaration of conformity referred to in Article 20, shall contain all of the following information:	Functional	intersects with	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	5	
Annex 4.1	N/A	Name and type and any additional information enabling the unique identification of the product with digital elements;	Functional	intersects with	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	5	
Annex 4.2	N/A	Name and address of the manufacturer or his authorised representative;	Functional	intersects with	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Annex 4.3	N/A	A statement that the EU declaration of conformity is issued under the sole responsibility of the provider;	Functional	intersects with	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	5	
Annex 4.4	N/A	Object of the declaration (identification of the product allowing traceability. It may include a photograph, where appropriate);	Functional	intersects with	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	5	
Annex 4.5	N/A	A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation;	Functional	intersects with	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	5	
Annex 4.6	N/A	References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared;	Functional	intersects with	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	5	
Annex 4.7	N/A	Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed and identification of the certificate issued;	Functional	intersects with	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	5	
Annex 4.8	N/A	Additional information:	Functional	intersects with	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	5	
Annex 5	Contents of The Technical Documentation	The technical documentation referred to in Article 23 shall contain at least the following information, as applicable to the relevant product with digital elements:	Functional	subset of	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Assets, Applications & Services (AAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	10	
Annex 5.1	N/A	a general description of the product with digital elements, including:	Functional	subset of	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Assets, Applications & Services (AAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	10	
Annex 5.1(a)	N/A	its intended purpose;	Functional	subset of	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Assets, Applications & Services (AAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	10	
Annex 5.1(b)	N/A	versions of software affecting compliance with essential requirements;	Functional	subset of	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Assets, Applications & Services (AAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	10	
Annex 5.1(c)	N/A	where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout;	Functional	subset of	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Assets, Applications & Services (AAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	10	
Annex 5.1(d)	N/A	user information and instructions as set out in Annex II;	Functional	subset of	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Assets, Applications & Services (AAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	10	
Annex 5.2	N/A	a description of the design, development and production of the product and vulnerability handling processes, including:	Functional	subset of	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Assets, Applications & Services (AAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	10	
Annex 5.2(a)	N/A	complete information on the design and development of the product with digital elements, including, where applicable, drawings and schemes and/or a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing;	Functional	subset of	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Assets, Applications & Services (AAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	10	
Annex 5.2(b)	N/A	complete information and specifications of the vulnerability handling processes put in place by the manufacturer, including the software bill of materials, the coordinated vulnerability disclosure policy, evidence of the provision of a contact address for the reporting of the vulnerabilities and a description of the technical solutions chosen for the secure distribution of updates;	Functional	subset of	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Assets, Applications & Services (AAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	10	
Annex 5.2(c)	N/A	complete information and specifications of the production and monitoring processes of the product with digital elements and the validation of these processes.	Functional	subset of	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Assets, Applications & Services (AAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	10	
Annex 5.3	N/A	an assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained as laid down in Article 10 of this Regulation;	Functional	subset of	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Assets, Applications & Services (AAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	10	
Annex 5.4	N/A	a list of the harmonised standards applied in full or in part the references of which have been published in the Official Journal of the European Union, common specifications as set out in Article 19 of this Regulation or cybersecurity certification schemes under Regulation (EU) 2019/881 pursuant to Article 18(3), and, where those harmonised standards, common specifications or cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential requirements set out in Sections 1 and 2 of Annex I, including a list of other relevant technical specifications applied. In the event of partly applied harmonised standards, common specifications or cybersecurity certifications, the technical documentation shall specify the parts which have been applied;	Functional	subset of	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Assets, Applications & Services (AAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	10	
Annex 5.5	N/A	reports of the tests carried out to verify the conformity of the product and of the vulnerability handling processes with the applicable essential requirements as set out in Sections 1 and 2 of Annex I;	Functional	subset of	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Assets, Applications & Services (AAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	10	
Annex 5.6	N/A	a copy of the EU declaration of conformity;	Functional	subset of	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Assets, Applications & Services (AAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	10	
Annex 5.7	N/A	where applicable, the software bill of materials as defined in Article 3, point (36), further to a reasoned request from a market surveillance authority provided that it is necessary in order for this authority to be able to check compliance with the essential requirements set out in Annex I.	Functional	subset of	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Assets, Applications & Services (AAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	10	
Annex 6	Conformity Assessment Procedures	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module A	Conformity Assessment procedure based on internal control (based on Module A)	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module A.1	N/A	Internal control is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2, 3 and 4, and ensures and declares on its sole responsibility that the products with digital elements satisfy all the essential requirements set out in Section 1 of Annex I and the manufacturer meets the essential requirements set out in Section 2 of Annex I.	Functional	subset of	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	10	
Annex 6 Module A.2	N/A	The manufacturer shall draw up the technical documentation described in Annex V.	Functional	intersects with	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for Assets, Applications & Services (AAS) in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	5	
Annex 6 Module A.3	N/A	Design, development, production and vulnerability handling of products with digital elements. The manufacturer shall take all measures necessary so that the design, development, production and vulnerability handling processes and their monitoring ensure compliance of the manufactured or developed products with digital elements and of the processes put in place by the manufacturer with the essential requirements set out in sections 1 and 2 of Annex I.	Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Annex 6 Module A.3	N/A	Design, development, production and vulnerability handling of products with digital elements. The manufacturer shall take all measures necessary so that the design, development, production and vulnerability handling processes and their monitoring ensure compliance of the manufactured or developed products with digital elements and of the processes put in place by the manufacturer with the essential requirements set out in sections 1 and 2 of Annex I.	Functional	intersects with	Minimum Viable Product (MVP) Security Requirements	TDA-02	Mechanisms exist to design, develop and produce Assets, Applications & Services (AAS) in such a way that risk-based technical and functional specifications ensure Minimum Viable Product (MVP) criteria establish an appropriate level of security and resiliency based on applicable risks and threats.	8	
Annex 6 Module A.4	N/A	Conformity marking and declaration of conformity	Functional	intersects with	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	5	
Annex 6 Module A.4.1	N/A	The manufacturer shall affix the CE to each individual product with digital elements that satisfies the applicable requirements of this Regulation.	Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
Annex 6 Module A.4.2	N/A	The manufacturer shall draw up a written EU declaration of conformity for each product with digital elements in accordance with Article 20 and keep it together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market. The EU declaration of conformity shall identify the product with digital elements for which it has been drawn up. A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.	Functional	intersects with	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	5	
Annex 6 Module A.5	Authorised representatives	The manufacturer's obligations set out in point 4 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.	Functional	intersects with	Localized Representation	CPL-08	Mechanisms exist to appoint localized representation with a physical presence in localities, as required by applicable laws and/or regulations.	5	
Annex 6 Module A.5	Authorised representatives	The manufacturer's obligations set out in point 4 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.	Functional	intersects with	Representative Powers	CPL-08.1	Mechanisms exist to contract localized representation to perform specified functions in regard to representing statutory and/or regulatory compliance matters.	5	
Annex 6 Module B	EU-type examination (based on Module B)	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module B.1	N/A	EU-type examination is the part of a conformity assessment procedure in which a notified body examines the technical design and development of a product and the vulnerability handling processes put in place by the manufacturer, and attests that a product with digital elements meets the essential requirements set out in Section 1 of Annex I and that the manufacturer meets the essential requirements set out in Section 2 of Annex I.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module B.2	N/A	EU-type examination shall be carried out by assessment of the adequacy of the technical design and development of the product through examination of the technical documentation and supporting evidence referred to in point 3, plus examination of specimens of one or more critical parts of the product (combination of production type and design type).	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module B.3	N/A	The manufacturer shall lodge an application for EU-type examination with a single notified body of his choice. The application shall include: - the name and address of the manufacturer and, if the application is lodged by the authorised representative, his name and address as well; - a written declaration that the same application has not been lodged with any other notified body; - the technical documentation, which shall make it possible to assess the product's conformity with the applicable essential requirements as set out in Section 1 of Annex I and the manufacturer's vulnerability handling processes set out in Section 2 of Annex I, and shall include an adequate analysis and assessment of the risk(s). The technical documentation shall specify the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and operation of the product. The technical documentation shall contain, wherever applicable, at least the elements set out in Annex V; - the supporting evidence for the adequacy of the technical design and development solutions and vulnerability handling processes. This supporting evidence shall mention any documents that have been used, in particular where the relevant harmonised standards and/or technical specifications have not been applied in full. The supporting evidence shall include, where necessary, the results of tests carried out by the appropriate laboratory of the manufacturer, or by another testing laboratory on his behalf and under his responsibility.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module B.4	N/A	The notified body shall:	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module B.4.1	N/A	examine the technical documentation and supporting evidence to assess the adequacy of the technical design and development of the product with the essential requirements set out in Section 1 of Annex I and of the vulnerability handling processes put in place by the manufacturer with the essential requirements set out in Section 2 of Annex I;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module B.4.2	N/A	verify that the specimen(s) have been developed or manufactured in conformity with the technical documentation, and identify the elements which have been designed and developed in accordance with the applicable provisions of the relevant harmonised standards and/or technical specifications, as well as the elements which have been designed and developed without applying the relevant provisions of those standards;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module B.4.3	N/A	carry out appropriate examinations and tests, or have them carried out, to check whether, where the manufacturer has chosen to apply the solutions in the relevant harmonised standards and/or technical specifications for the requirements set out in Annex I, these have been applied correctly;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module B.4.4	N/A	carry out appropriate examinations and tests, or have them carried out, to check whether, where the solutions in the relevant harmonised standards and/or technical specifications for the requirements set out in Annex I have not been applied, the solutions adopted by the manufacturer meet the corresponding essential requirements;	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module B.4.5	N/A	agree with the manufacturer on a location where the examinations and tests will be carried out.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module B.5	N/A	The notified body shall draw up an evaluation report that records the activities undertaken in accordance with point 4 and their outcomes. Without prejudice to its obligations vis-à-vis the notifying authorities, the notified body shall release the content of that report, in full or in part, only with the agreement of the manufacturer.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module B.6	N/A	Where the type and the vulnerability handling processes meet the essential requirements set out in Annex I, the notified body shall issue an EU-type examination certificate to the manufacturer. The certificate shall contain the name and address of the manufacturer, the conclusions of the examination, the conditions (if any) for its validity and the necessary data for identification of the approved type and vulnerability handling processes. The certificate may have one or more annexes attached. The certificate and its annexes shall contain all relevant information to allow the conformity of manufactured or developed products with the examined type and vulnerability handling processes to be evaluated and to allow for in-service control. Where the type and the vulnerability handling processes do not satisfy the applicable essential requirements set out in Annex I, the notified body shall refuse to issue an EU-type examination certificate and shall inform the applicant accordingly, giving detailed reasons for its refusal.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	

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)
Annex 6 Module B.7	N/A	The notified body shall keep itself apprised of any changes in the generally acknowledged state of the art which indicate that the approved type and the vulnerability handling processes may no longer comply with the applicable essential requirements set out in Annex I to this Regulation, and shall determine whether such changes require further investigation. If so, the notified body shall inform the manufacturer accordingly. The manufacturer shall inform the notified body that holds the technical documentation relating to the EU-type examination certificate of all modifications to the approved type and the vulnerability handling processes that may affect the conformity with the essential requirements set out in Annex I, or the conditions for validity of the certificate. Such modifications shall require additional approval in the form of an addition to the original EU-type examination certificate.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module B.8	N/A	Each notified body shall inform its notifying authorities concerning the EU-type examination certificates and/or any additions thereto which it has issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of certificates and/or any additions thereto refused, suspended or otherwise restricted. Each notified body shall inform the other notified bodies concerning the EU-type examination certificates and/or any additions thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, concerning the certificates and/or additions thereto which it has issued. The Commission, the Member States and the other notified bodies may, on request, obtain a copy of the EU-type examination certificates and/or additions thereto. On request, the Commission and the Member States may obtain a copy of the technical documentation and the results of the examinations carried out by the notified body. The notified body shall keep a copy of the EU-type examination certificate, its annexes and additions, as well as the technical file including the documentation submitted by the manufacturer, until the expiry of the validity of the certificate.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module B.9	N/A	The manufacturer shall keep a copy of the EU-type examination certificate, its annexes and additions together with the technical documentation at the disposal of the national authorities for 10 years after the product has been placed on the market.	Functional	subset of	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	10	
Annex 6 Module B.10	N/A	The manufacturer's authorised representative may lodge the application referred to in point 3 and fulfil the obligations set out in points 7 and 9, provided that they are specified in the mandate.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module C	Conformity to type based on internal production control (based on Module C)	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module C.1	N/A	Conformity to type based on internal production control is the part of a conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2 and 3, and ensures and declares that the products concerned are in conformity with the type described in the EU-type examination certificate and satisfy the essential requirements set out in Section 1 of Annex I.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module C.2	Production	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module C.2.1	N/A	The manufacturer shall take all measures necessary so that the production and its monitoring ensure conformity of the manufactured products with the approved type described in the EU-type examination certificate and with the essential requirements as set out in Section 1 of Annex I.	Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
Annex 6 Module C.3	Conformity marking and declaration of conformity	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module C.3.1	N/A	The manufacturer shall affix the CE marking to each individual product that is in conformity with the type described in the EU-type examination certificate and satisfies the applicable requirements of the legislative instrument.	Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
Annex 6 Module C.3.2	N/A	The manufacturer shall draw up a written declaration of conformity for a product model and keep it at the disposal of the national authorities for 10 years after the product has been placed on the market. The declaration of conformity shall identify the product model for which it has been drawn up. A copy of the declaration of conformity shall be made available to the relevant authorities upon request.	Functional	intersects with	Declaration of Conformity	CPL-01.5	Mechanisms exist to generate a declaration of conformity for each conformity assessment, where the document: (1) Is concise; (2) Unambiguously reflects the current status; (3) Is physically or electronically signed; and (4) Where possible, is machine readable.	5	
Annex 6 Module C.3.2	N/A	The manufacturer shall draw up a written declaration of conformity for a product model and keep it at the disposal of the national authorities for 10 years after the product has been placed on the market. The declaration of conformity shall identify the product model for which it has been drawn up. A copy of the declaration of conformity shall be made available to the relevant authorities upon request.	Functional	intersects with	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	8	
Annex 6 Module C.4	Authorised representative	The manufacturer's obligations set out in point 3 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.	Functional	intersects with	Localized Representation	CPL-08	Mechanisms exist to appoint localized representation with a physical presence in localities, as required by applicable laws and/or regulations.	5	
Annex 6 Module C.4	Authorised representative	The manufacturer's obligations set out in point 3 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.	Functional	intersects with	Representative Powers	CPL-08.1	Mechanisms exist to contract localized representation to perform specified functions in regard to representing statutory and/or regulatory compliance matters.	5	
Annex 6 Module H	Conformity based on full quality assurance (based on Module H)	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module H.1	N/A	Conformity based on full quality assurance is the conformity assessment procedure whereby the manufacturer fulfils the obligations laid down in points 2 and 5, and ensures and declares on his sole responsibility that the products (or product categories) concerned satisfy the essential requirements set out in Section 1 of Annex I, and that the vulnerability handling processes put in place by the manufacturer meet the requirements set out in Section 2 of Annex I.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module H.2	N/A	Design, development, production and vulnerability handling of products with digital elements. The manufacturer shall operate an approved quality system as specified in point 3 for the design, development, and production of the products concerned and for handling vulnerabilities, maintain its effectiveness throughout the lifecycle of the products concerned, and shall be subject to surveillance as specified in point 4.	Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	8	
Annex 6 Module H.3	Quality system	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module H.3.1	N/A	The manufacturer shall lodge an application for assessment of his quality system with the notified body of his choice, for the products concerned. The application shall include: - the name and address of the manufacturer and, if the application is lodged by the authorised representative, his name and address as well; - the technical documentation for one model of each category of products intended to be manufactured or developed. The technical documentation shall, wherever applicable, contain at least the elements as set out in Annex V; - the documentation concerning the quality system; and - a written declaration that the same application has not been lodged with any other notified body.	Functional	intersects with	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate cybersecurity and data protection controls at planned intervals or when the system, service or project undergoes significant changes.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
Annex 6 Module H.3.2	N/A	The quality system shall ensure compliance of the products with the essential requirements set out in Section 1 of Annex I and compliance of the vulnerability handling processes put in place by the manufacturer with the requirements set out in Section 2 of Annex I. All the elements, requirements and provisions adopted by the manufacturer shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions. That quality system documentation shall permit a consistent interpretation of the quality programmes, plans, manuals and records. It shall, in particular, contain an adequate description of: - the quality objectives and the organisational structure, responsibilities and powers of the management with regard to design, development, product quality and vulnerability handling; - the technical design and development specifications, including standards, that will be applied and, where the relevant harmonised standards and/or technical specifications will not be applied in full, the means that will be used to ensure that the essential requirements set out in Section 1 of Annex I that apply to the products will be met; - the procedural specifications, including standards, that will be applied and, where the relevant harmonised standards and/or technical specifications will not be applied in full, the means that will be used to ensure that the essential requirements set out in Section 2 of Annex I that apply to the manufacturer will be met; - the design and development control, as well as design and development verification techniques, processes and systematic actions that will be used when designing and developing the products pertaining to the product category covered; - the corresponding production, quality control and quality assurance techniques, processes and systematic actions that will be used; - the examinations and tests that will be carried out before, during and after production, and the frequency with which they will be carried out;	Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	8	
Annex 6 Module H.3.3	N/A	The notified body shall assess the quality system to determine whether it satisfies the requirements referred to in point 3.2. It shall presume conformity with those requirements in respect of the elements of the quality system that comply with the corresponding specifications of the national standard that implements the relevant harmonised standard and/or technical specification. In addition to experience in quality management systems, the auditing team shall have at least one member experienced as an assessor in the relevant product field and product technology concerned, and knowledge of the applicable requirements of this Regulation. The audit shall include an assessment visit to the manufacturer's premises, where such premises exist. The auditing team shall review the technical documentation referred to in point 3.1, second indent, to verify the manufacturer's ability to identify the applicable requirements of this Regulation and to carry out the necessary examinations with a view to ensuring compliance of the product with those requirements. The manufacturer or his authorised representative shall be notified of the decision. The notification shall contain the conclusions of the audit and the reasoned assessment decision.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module H.3.4	N/A	The manufacturer shall undertake to fulfil the obligations arising out of the quality system as approved and to maintain it so that it remains adequate and efficient.	Functional	subset of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
Annex 6 Module H.3.5	N/A	The manufacturer shall keep the notified body that has approved the quality system informed of any intended change to the quality system. The notified body shall evaluate any proposed changes and decide whether the modified quality system will continue to satisfy the requirements referred to in point 3.2 or whether a reassessment is necessary. It shall notify the manufacturer of its decision. The notification shall contain the conclusions of the examination and the reasoned assessment decision.	Functional	intersects with	Independent Assessors	CPL-03.1	Mechanisms exist to utilize independent assessors to evaluate cybersecurity and data protection controls at planned intervals or when the system, service or project undergoes significant changes.	3	
Annex 6 Module H.4	Surveillance under the responsibility of the notified body	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module H.4.1	N/A	The purpose of surveillance is to make sure that the manufacturer duly fulfils the obligations arising out of the approved quality system.	Functional	Functional	No relationship	N/A	N/A	No applicable SCF control	
Annex 6 Module H.4.2	N/A	The manufacturer shall, for assessment purposes, allow the notified body access to the design, development, production, inspection, testing and storage sites, and shall provide it with all necessary information, in particular: - the quality system documentation; - the quality records as provided for by the design part of the quality system, such as results of analyses, calculations, tests, etc.; - the quality records as provided for by the manufacturing part of the quality system, such as inspection reports and test data, calibration data, qualification reports on the personnel concerned, etc.	Functional	subset of	Assessor Access	CPL-03.3	Mechanisms exist to grant assessors minimum necessary access to conduct conformity assessments, including: (1) Logical access to design, development, production, inspection and testing artifacts; and (2) Physical access to facilities.	10	
Annex 6 Module H.4.3	N/A	The notified body shall carry out periodic audits to make sure that the manufacturer maintains and applies the quality system and shall provide the manufacturer with an audit report.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module H.5	Conformity marking and declaration of conformity	N/A	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module H.5.1	N/A	The manufacturer shall affix the CE marking, and, under the responsibility of the notified body referred to in point 3.1, the latter's identification number to each individual product that satisfies the requirements set out in Section 1 of Annex I to this Regulation.	Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
Annex 6 Module H.5.2	N/A	The manufacturer shall draw up a written declaration of conformity for each product model and keep it at the disposal of the national authorities for 10 years after the product has been placed on the market. The declaration of conformity shall identify the product model for which it has been drawn up. A copy of the declaration of conformity shall be made available to the relevant authorities upon request.	Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
Annex 6 Module H.6	N/A	The manufacturer shall, for a period ending at least 10 years after the product has been placed on the market, keep at the disposal of the national authorities: - the technical documentation referred to in point 3.1; - the documentation concerning the quality system referred to in point 3.1; - the change referred to in point 3.5, as approved; - the decisions and reports of the notified body referred to in points 3.5, 4.3 and 4.4.	Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Assets, Applications & Services (AAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
Annex 6 Module H.7	N/A	Each notified body shall inform its notifying authorities of quality system approvals issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of quality system approvals refused, suspended or otherwise restricted. Each notified body shall inform the other notified bodies of quality system approvals which it has refused, suspended or withdrawn, and, upon request, of quality system approvals which it has issued.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
Annex 6 Module H.8	Authorised representative	The manufacturer's obligations set out in points 3.1, 3.5, 5 and 6 may be fulfilled by his authorised representative, on his behalf and under his responsibility, provided that they are specified in the mandate.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	