Set Theory Relationship Mapping (STRM)

Reference Document : **Secure Controls Framework (SCF) version 2024.2**
Focal Document: **Digital Operational Resilience Act (DORA)**
Focal Document URL: **https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554&from=EN**
STRM URL: **https://content.securecontrolsframework.com/strm/scf-2024-2-dora.pdf**

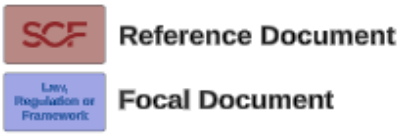
Set Theory Relationship Mapping (STRM) is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). STRM also allows the strength of the mapping to be captured.

STRM relies on a justification for the relationship claim. There are three (3) options for the rationale, which is a high-level context within which the two concepts are related:

1. **Syntactic**: How similar is the wording that expresses the two concepts? This is a word-for-word analysis of the relationship, not an interpretation of the language.
2. **Semantic**: How similar are the meanings of the two concepts? This involves some interpretation of each concept's language.
3. **Functional**: How similar are the results of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise executed.

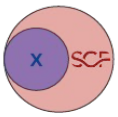
Based on NIST IR 8477, STRM supports five (5) five relationship types to describe the logical similarity between two distinct concepts:

1. **Subset Of**
2. **Intersects With**
3. **Equal**
4. **Superset Of**
5. **No Relationship**

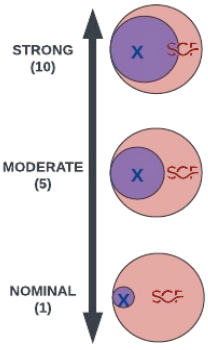


Relationship Type #1:
SUBSET OF

Focal Document Element is a subset of SCF control. In other words, SCF control contains everything that Focal Document Element does and more.

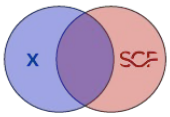


SUBSET OF
Relative Relationship Strength (control versus control)

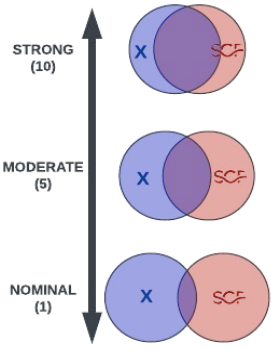


Relationship Type #2:
INTERSECTS WITH

SCF control has some overlap with Focal Document Element, but each includes content that the other does not.

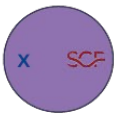


INTERSECTS WITH
Relative Relationship Strength (control versus control)

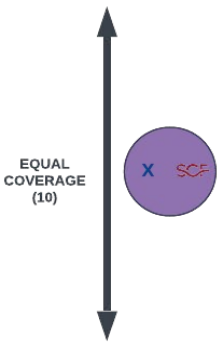


Relationship Type #3:
EQUAL

SCF control and Focal Document Element are the same, although not necessarily identical.

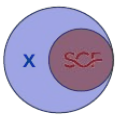


EQUAL
Relative Relationship Strength (control versus control)

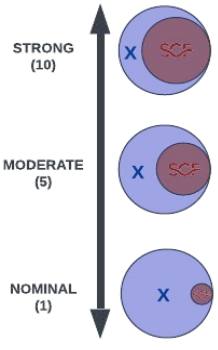


Relationship Type #4:
SUPERSET OF

Focal Document Element is a superset of SCF control. In other words, Focal Document Element contains everything that SCF control does and more.

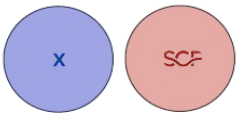


SUPERSET OF
Relative Relationship Strength (control versus control)

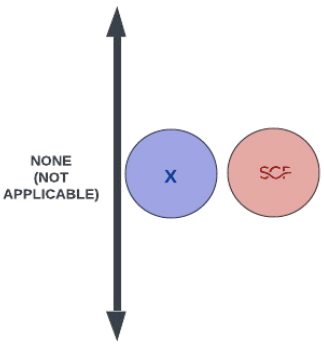


Relationship Type #5:
NO RELATIONSHIP

SCF control and Focal Document Element are unrelated; their content does not overlap.



NO RELATIONSHIP
Relative Relationship Strength (control versus control)



FDE #	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 4.1	Financial entities shall implement the rules laid down in Chapter II in accordance with the principle of proportionality, taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations.	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 4.2	In addition, the application by financial entities of Chapters III, IV and V, Section I, shall be proportionate to their size and overall risk profile, and to the nature, scale and complexity of their services, activities and operations, as specifically provided for in the relevant rules of those Chapters.	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 4.3	The competent authorities shall consider the application of the proportionality principle by financial entities when reviewing the consistency of the ICT risk management framework on the basis of the reports submitted upon the request of competent authorities pursuant to Article 6(5) and Article 16(2).	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 5.1	Financial entities shall have in place an internal governance and control framework that ensures an effective and prudent management of ICT risk, in accordance with Article 6(4), in order to achieve a high level of digital operational resilience.	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
Article 5.2	The management body of the financial entity shall define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework referred to in Article 6(1). For the purposes of the first subparagraph, the management body shall:	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
		Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
Article 5.2(a)	bear the ultimate responsibility for managing the financial entity's ICT risk;	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
		Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
Article 5.2(b)	put in place policies that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality, of data;	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
		Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
Article 5.2(c)	set clear roles and responsibilities for all ICT-related functions and establish appropriate governance arrangements to ensure effective and timely communication, cooperation and coordination among those functions;	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
		Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
		Functional	intersects with	Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity responsibilities for all personnel.	5	
Article 5.2(d)	bear the overall responsibility for setting and approving the digital operational resilience strategy as referred to in Article 6(8), including the determination of the appropriate risk tolerance level of ICT risk of the financial entity, as referred to in Article 6(8), point (b);	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
		Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
Article 5.2(e)	approve, oversee and periodically review the implementation of the financial entity's ICT business continuity policy and ICT response and recovery plans, referred to, respectively, in Article 11(1) and (3), which may be adopted as a dedicated specific policy forming an integral part of the financial entity's overall business continuity policy and response and recovery plan;	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
		Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
Article 5.2(f)	approve and periodically review the financial entity's ICT internal audit plans, ICT audits and material modifications to them;	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
		Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
Article 5.2(g)	allocate and periodically review the appropriate budget to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including relevant ICT security awareness programmes and digital operational resilience training referred to in Article 13(6), and ICT skills for all staff;	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
		Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
Article 5.2(h)	approve and periodically review the financial entity's policy on arrangements regarding the use of ICT services provided by ICT third-party service providers;	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
		Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
Article 5.2(i)	put in place, at corporate level, reporting channels enabling it to be duly informed of the following:	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
Article 5.2(i)(i)	arrangements concluded with ICT third-party service providers on the use of ICT services,	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
		Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
Article 5.2(i)(ii)	any relevant planned material changes regarding the ICT third-party service providers,	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
		Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
Article 5.2(i)(iii)	the potential impact of such changes on the critical or important functions subject to those arrangements, including a risk analysis summary to assess the impact of those changes, and at least major ICT-related incidents and their impact, as well as response, recovery and corrective measures.	Functional	intersects with	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, data protection and business alignment through a steering committee or advisory board, comprised of key cybersecurity, data privacy and business executives, which meets formally and on a regular basis.	5	
		Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
Article 5.3	Financial entities, other than microenterprises, shall establish a role in order to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services, or shall designate a member of senior management as responsible for overseeing the related risk exposure and relevant documentation.	Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	

FDE #	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 5.4	Members of the management body of the financial entity shall actively keep up to date with sufficient knowledge and skills to understand and assess ICT risk and its impact on the operations of the financial entity, including by following specific training on a regular basis, commensurate to the ICT risk being managed.	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
Article 6.1	Financial entities shall have a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system, which enables them to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 6.2	The ICT risk management framework shall include at least strategies, policies, procedures, ICT protocols and tools that are necessary to duly and adequately protect all information assets and ICT assets, including computer software, hardware, servers, as well as to protect all relevant physical components and infrastructures, such as premises, data centres and sensitive designated areas, to ensure that all information assets and ICT assets are adequately protected from risks including damage and unauthorised access or usage.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
		Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
		Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 6.3	In accordance with their ICT risk management framework, financial entities shall minimise the impact of ICT risk by deploying appropriate strategies, policies, procedures, ICT protocols and tools. They shall provide complete and updated information on ICT risk and on their ICT risk management framework to the competent authorities upon their request.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 6.4	Financial entities, other than microenterprises, shall assign the responsibility for managing and overseeing ICT risk to a control function and ensure an appropriate level of independence of such control function in order to avoid conflicts of interest. Financial entities shall ensure appropriate segregation and independence of ICT risk management functions, control functions, and internal audit functions, according to the three lines of defence model, or an internal risk management and control model.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 6.5	The ICT risk management framework shall be documented and reviewed at least once a year, or periodically in the case of microenterprises, as well as upon the occurrence of major ICT-related incidents, and following supervisory instructions or conclusions derived from relevant digital operational resilience testing or audit processes. It shall be continuously improved on the basis of lessons derived from implementation and monitoring. A report on the review of the ICT risk management framework shall be submitted to the competent authority upon its request.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 6.6	The ICT risk management framework of financial entities, other than microenterprises, shall be subject to internal audit by auditors on a regular basis in line with the financial entities' audit plan. Those auditors shall possess sufficient knowledge, skills and expertise in ICT risk, as well as appropriate independence. The frequency and focus of ICT audits shall be commensurate to the ICT risk of the financial entity.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 6.7	Based on the conclusions from the internal audit review, financial entities shall establish a formal follow-up process, including rules for the timely verification and remediation of critical ICT audit findings.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 6.8	The ICT risk management framework shall include a digital operational resilience strategy setting out how the framework shall be implemented. To that end, the digital operational resilience strategy shall include methods to address ICT risk and attain specific ICT objectives, by:	Functional	intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity & data privacy-specific business plan and set of objectives to achieve that plan.	5	
		Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 6.8(a)	explaining how the ICT risk management framework supports the financial entity's business strategy and objectives;	Functional	intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity & data privacy-specific business plan and set of objectives to achieve that plan.	5	
		Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 6.8(b)	establishing the risk tolerance level for ICT risk, in accordance with the risk appetite of the financial entity, and analysing the impact tolerance for ICT disruptions;	Functional	intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity & data privacy-specific business plan and set of objectives to achieve that plan.	5	
		Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 6.8(c)	setting out clear information security objectives, including key performance indicators and key risk metrics;	Functional	intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity & data privacy-specific business plan and set of objectives to achieve that plan.	5	
		Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 6.8(d)	explaining the ICT reference architecture and any changes needed to reach specific business objectives;	Functional	intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity & data privacy-specific business plan and set of objectives to achieve that plan.	5	
		Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 6.8(e)	outlining the different mechanisms put in place to detect ICT-related incidents, prevent their impact and provide protection from it;	Functional	intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity & data privacy-specific business plan and set of objectives to achieve that plan.	5	
		Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 6.8(f)	evidencing the current digital operational resilience situation on the basis of the number of major ICT-related incidents reported and the effectiveness of preventive measures;	Functional	intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity & data privacy-specific business plan and set of objectives to achieve that plan.	5	
		Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 6.8(g)	implementing digital operational resilience testing, in accordance with Chapter IV of this Regulation;	Functional	intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity & data privacy-specific business plan and set of objectives to achieve that plan.	5	
		Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 6.8(h)	outlining a communication strategy in the event of ICT-related incidents the disclosure of which is required in accordance with Article 14.	Functional	intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity & data privacy-specific business plan and set of objectives to achieve that plan.	5	
		Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 6.9	Financial entities may, in the context of the digital operational resilience strategy referred to in paragraph 8, define a holistic ICT multi-vendor strategy, at group or entity level, showing key dependencies on ICT third-party service providers and explaining the rationale behind the procurement mix of ICT third-party service providers.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 6.10	Financial entities may, in accordance with Union and national sectoral law, outsource the tasks of verifying compliance with ICT risk management requirements to intra-group or external undertakings. In case of such outsourcing, the financial entity remains fully responsible for the verification of compliance with the ICT risk management requirements.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 7	In order to address and manage ICT risk, financial entities shall use and maintain updated ICT systems, protocols and tools that are:	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
Article 7(a)	appropriate to the magnitude of operations supporting the conduct of their activities, in accordance with the proportionality principle as referred to in Article 4;	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
		Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
		Functional	intersects with	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
		Functional	intersects with	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required cybersecurity & data privacy controls for each system, application and/or service under their control are implemented correctly and are operating as intended.	5	
		Functional	intersects with	Authorize Systems, Applications & Services	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each system, application and/or service under their control.	5	
		Functional	intersects with	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor systems, applications and/or services under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity & data privacy controls are operating as intended.	5	
		Functional	subset of	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	10	
		Functional	intersects with	Cybersecurity & Data Privacy Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity & data privacy programs and document all exceptions to this requirement.	5	
		Functional	intersects with	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects / initiatives.	5	

FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
		Functional	intersects with	Cybersecurity & Data Privacy In Project Management	PRM-04	Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
		Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
		Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
Article 7(b)	reliable;	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
		Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
		Functional	intersects with	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
		Functional	intersects with	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required cybersecurity & data privacy controls for each system, application and/or service under their control are implemented correctly and are operating as intended.	5	
		Functional	intersects with	Authorize Systems, Applications & Services	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each system, application and/or service under their control.	5	
		Functional	intersects with	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor systems, applications and/or services under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity & data privacy controls are operating as intended.	5	
		Functional	intersects with	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	5	
		Functional	intersects with	Cybersecurity & Data Privacy Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity & data privacy programs and document all exceptions to this requirement.	5	
		Functional	intersects with	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects / initiatives.	5	
		Functional	intersects with	Cybersecurity & Data Privacy In Project Management	PRM-04	Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
		Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
		Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
Article 7(c)	equipped with sufficient capacity to accurately process the data necessary for the performance of activities and the timely provision of services, and to deal with peak orders, message or transaction volumes, as needed, including where new technology is introduced;	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
		Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
		Functional	intersects with	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
		Functional	intersects with	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required cybersecurity & data privacy controls for each system, application and/or service under their control are implemented correctly and are operating as intended.	5	
		Functional	intersects with	Authorize Systems, Applications & Services	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each system, application and/or service under their control.	5	
		Functional	intersects with	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor systems, applications and/or services under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity & data privacy controls are operating as intended.	5	
		Functional	subset of	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	10	
		Functional	intersects with	Cybersecurity & Data Privacy Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity & data privacy programs and document all exceptions to this requirement.	5	
		Functional	intersects with	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects / initiatives.	5	
		Functional	intersects with	Cybersecurity & Data Privacy In Project Management	PRM-04	Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
		Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
		Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
Article 7(d)	technologically resilient in order to adequately deal with additional information processing needs as required under stressed market conditions or other adverse situations.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
		Functional	intersects with	Select Controls	GOV-15.1	Mechanisms exist to compel data and/or process owners to select required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
		Functional	intersects with	Implement Controls	GOV-15.2	Mechanisms exist to compel data and/or process owners to implement required cybersecurity & data privacy controls for each system, application and/or service under their control.	5	
		Functional	intersects with	Assess Controls	GOV-15.3	Mechanisms exist to compel data and/or process owners to assess if required cybersecurity & data privacy controls for each system, application and/or service under their control are implemented correctly and are operating as intended.	5	
		Functional	intersects with	Authorize Systems, Applications & Services	GOV-15.4	Mechanisms exist to compel data and/or process owners to obtain authorization for the production use of each system, application and/or service under their control.	5	
		Functional	intersects with	Monitor Controls	GOV-15.5	Mechanisms exist to compel data and/or process owners to monitor systems, applications and/or services under their control on an ongoing basis for applicable threats and risks, as well as to ensure cybersecurity & data privacy controls are operating as intended.	5	
		Functional	intersects with	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	5	

FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
		Functional	intersects with	Cybersecurity & Data Privacy Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity & data privacy programs and document all exceptions to this requirement.	5	
		Functional	intersects with	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects / initiatives.	5	
		Functional	intersects with	Cybersecurity & Data Privacy In Project Management	PRM-04	Mechanisms exist to assess cybersecurity & data privacy controls in system project development to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the requirements.	5	
		Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
		Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
Article 8.1	As part of the ICT risk management framework referred to in Article 6(1), financial entities shall identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk. Financial entities shall review as needed, and at least yearly, the adequacy of this classification and of any relevant documentation.	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: • The resulting risk to organizational operations, assets, individuals and other organizations; and • Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
Article 8.2	Financial entities shall, on a continuous basis, identify all sources of ICT risk, in particular the risk exposure to and from other financial entities, and assess cyber threats and ICT vulnerabilities relevant to their ICT supported business functions, information assets and ICT assets. Financial entities shall review on a regular basis, and at least yearly, the risk scenarios impacting them.	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: • Assumptions affecting risk assessments, risk response and risk monitoring; • Constraints affecting risk assessments, risk response and risk monitoring; • The organizational risk tolerance; and • Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
		Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
Article 8.3	Financial entities, other than microenterprises, shall perform a risk assessment upon each major change in the network and information system infrastructure, in the processes or procedures affecting their ICT supported business functions, information assets or ICT assets.	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
Article 8.4	Financial entities shall identify all information assets and ICT assets, including those on remote sites, network resources and hardware equipment, and shall map those considered critical. They shall map the configuration of the information assets and ICT assets and the links and interdependencies between the different information assets and ICT assets.	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: • Accurately reflects the current systems, applications and services in use; • Identifies authorized software products, including business justification details; • Is at the level of granularity deemed necessary for tracking and reporting; • Includes organization-defined information deemed necessary to achieve effective property accountability; and • Is available for review and audit by designated organizational personnel.	5	
		Functional	intersects with	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: • Contain sufficient detail to assess the security of the network's architecture; • Reflect the current architecture of the network environment; and • Document all sensitive/regulated data flows.	5	
		Functional	intersects with	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical systems, applications and services that support essential missions and business functions.	5	
		Functional	intersects with	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
Article 8.5	Financial entities shall identify and document all processes that are dependent on ICT third-party service providers, and shall identify interconnections with ICT third-party service providers that provide services that support critical or important functions.	Functional	intersects with	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of technology assets that support more than one critical business function.	5	
Article 8.6	For the purposes of paragraphs 1, 4 and 5, financial entities shall maintain relevant inventories and update them periodically and every time any major change as referred to in paragraph 3 occurs.	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: • Accurately reflects the current systems, applications and services in use; • Identifies authorized software products, including business justification details; • Is at the level of granularity deemed necessary for tracking and reporting; • Includes organization-defined information deemed necessary to achieve effective property accountability; and • Is available for review and audit by designated organizational personnel.	5	
		Functional	intersects with	Updates During Installations / Removals	AST-02.1	Mechanisms exist to update asset inventories as part of component installations, removals and asset upgrades.	5	
Article 8.7	Financial entities, other than microenterprises, shall on a regular basis, and at least yearly, conduct a specific ICT risk assessment on all legacy ICT systems and, in any case before and after connecting technologies, applications or systems.	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
		Functional	intersects with	Technical Debt Reviews	SEA-02.3	Mechanisms exist to conduct ongoing "technical debt" reviews of hardware and software technologies to remediate outdated and/or unsupported technologies.	5	
Article 9.1	For the purposes of adequately protecting ICT systems and with a view to organising response measures, financial entities shall continuously monitor and control the security and functioning of ICT systems and tools and shall minimise the impact of ICT risk on ICT systems through the deployment of appropriate ICT security tools, policies and procedures.	Functional	subset of	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	10	
		Functional	intersects with	Security Concept Of Operations (CONOPS)	OPS-02	Mechanisms exist to develop a security Concept of Operations (CONOPS), or a similarly-defined plan for achieving cybersecurity objectives, that documents management, operational and technical measures implemented to apply defense-in-depth techniques that is communicated to all appropriate stakeholders.	5	
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
Article 9.2	Financial entities shall design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit.	Functional	intersects with	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	5	
		Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
		Functional	intersects with	Security Concept Of Operations (CONOPS)	OPS-02	Mechanisms exist to develop a security Concept of Operations (CONOPS), or a similarly-defined plan for achieving cybersecurity objectives, that documents management, operational and technical measures implemented to apply defense-in-depth techniques that is communicated to all appropriate stakeholders.	5	

FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
		Functional	intersects with	Service Delivery (Business Process Support)	OPS-03	Mechanisms exist to define supporting business processes and implement appropriate governance and service management to ensure appropriate planning, delivery and support of the organization's technology capabilities supporting business functions, workforce, and/or customers based on industry-recognized standards to achieve the specific goals of the process area.	5	
Article 9.3	In order to achieve the objectives referred to in paragraph 2, financial entities shall use ICT solutions and processes that are appropriate in accordance with Article 4. Those ICT solutions and processes shall:	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
Article 9.3(a)	ensure the security of the means of transfer of data;	Functional	intersects with	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	5	
		Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
		Functional	intersects with	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	5	
		Functional	intersects with	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
		Functional	intersects with	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5	
Article 9.3(b)	minimise the risk of corruption or loss of data, unauthorised access and technical flaws that may hinder business activity;	Functional	intersects with	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	5	
		Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
		Functional	intersects with	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	5	
		Functional	intersects with	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
		Functional	intersects with	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5	
Article 9.3(c)	prevent the lack of availability, the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data;	Functional	intersects with	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	5	
		Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
		Functional	intersects with	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	5	
		Functional	intersects with	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
		Functional	intersects with	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5	
Article 9.3(d)	ensure that data is protected from risks arising from data management, including poor administration, processing- related risks and human error.	Functional	intersects with	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	5	
		Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
		Functional	intersects with	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	5	
		Functional	intersects with	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity & data privacy principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
		Functional	intersects with	Defense-In-Depth (DiD) Architecture	SEA-03	Mechanisms exist to implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.	5	
Article 9.4	As part of the ICT risk management framework referred to in Article 6(1), financial entities shall:	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
Article 9.4(a)	develop and document an information security policy defining rules to protect the availability, authenticity, integrity and confidentiality of data, information assets and ICT assets, including those of their customers, where applicable;	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
Article 9.4(b)	following a risk-based approach, establish a sound network and infrastructure management structure using appropriate techniques, methods and protocols that may include implementing automated mechanisms to isolate affected information assets in the event of cyber-attacks;	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
		Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
		Functional	intersects with	Automated Incident Handling Processes	IRO-02.1	Automated mechanisms exist to support the incident handling process.	5	
		Functional	intersects with	Automatic Disabling of System	IRO-02.6	Mechanisms exist to automatically disable systems, upon detection of a possible incident that meets organizational criteria, which allows for forensic analysis to be performed.	5	
Article 9.4(c)	implement policies that limit the physical or logical access to information assets and ICT assets to what is required for legitimate and approved functions and activities only, and establish to that end a set of policies, procedures and controls that address access rights and ensure a sound administration thereof;	Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
Article 9.4(d)	implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes;	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
		Functional	intersects with	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
Article 9.4(e)	implement documented policies, procedures and controls for ICT change management, including changes to software, hardware, firmware components, systems or security parameters, that are based on a risk assessment approach and are an integral part of the financial entity's overall change management process, in order to ensure that all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner;	Functional	subset of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
		Functional	intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	

FDE #	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 9.4(e)		Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
		Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
Article 9.4(f)	have appropriate and comprehensive documented policies for patches and updates.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	5	
		Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
		Functional	intersects with	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	5	
Article 9 (end)	For the purposes of the first subparagraph, point (b), financial entities shall design the network connection infrastructure in a way that allows it to be instantaneously severed or segmented in order to minimise and prevent contagion, especially for interconnected financial processes. For the purposes of the first subparagraph, point (e), the ICT change management process shall be approved by appropriate lines of management and shall have specific protocols in place.	Functional	subset of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
Article 10.1	Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Article 17, including ICT network performance issues and ICT-related incidents, and to identify potential material single points of failure. All detection mechanisms referred to in the first subparagraph shall be regularly tested in accordance with Article 25.	Functional	intersects with	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
Article 10.2	The detection mechanisms referred to in paragraph 1 shall enable multiple layers of control, define alert thresholds and criteria to trigger and initiate ICT-related incident response processes, including automatic alert mechanisms for relevant staff in charge of ICT-related incident response.	Functional	intersects with	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	
Article 10.3	Financial entities shall devote sufficient resources and capabilities to monitor user activity, the occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
Article 10.4	Data reporting service providers shall, in addition, have in place systems that can effectively check trade reports for completeness, identify omissions and obvious errors, and request re-transmission of those reports.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 11.1	As part of the ICT risk management framework referred to in Article 6(1) and based on the identification requirements set out in Article 8, financial entities shall put in place a comprehensive ICT business continuity policy, which may be adopted as a dedicated specific policy, forming an integral part of the overall business continuity policy of the financial entity.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
Article 11.2	Financial entities shall implement the ICT business continuity policy through dedicated, appropriate and documented arrangements, plans, procedures and mechanisms aiming to:	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
Article 11.2(a)	ensure the continuity of the financial entity's critical or important functions;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
Article 11.2(b)	quickly, appropriately and effectively respond to, and resolve, all ICT-related incidents in a way that limits damage and prioritises the resumption of activities and recovery actions;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
Article 11.2(c)	activate, without delay, dedicated plans that enable containment measures, processes and technologies suited to each type of ICT-related incident and prevent further damage, as well as tailored response and recovery procedures established in accordance with Article 12;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
Article 11.2(d)	estimate preliminary impacts, damages and losses;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
Article 11.2(e)	set out communication and crisis management actions that ensure that updated information is transmitted to all relevant internal staff and external stakeholders in accordance with Article 14, and report to the competent authorities in accordance with Article 19.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
Article 11.3	As part of the ICT risk management framework referred to in Article 6(1), financial entities shall implement associated ICT response and recovery plans which, in the case of financial entities other than microenterprises, shall be subject to independent internal audit reviews.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
Article 11.4	Financial entities shall put in place, maintain and periodically test appropriate ICT business continuity plans, notably with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
		Functional	intersects with	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
Article 11.5	As part of the overall business continuity policy, financial entities shall conduct a business impact analysis (BIA) of their exposures to severe business disruptions. Under the BIA, financial entities shall assess the potential impact of severe business disruptions by means of quantitative and qualitative criteria, using internal and external data and scenario analysis, as appropriate. The BIA shall consider the criticality of identified and mapped business functions, support processes, third-party dependencies and information assets, and their interdependencies. Financial entities shall ensure that ICT assets and ICT services are designed and used in full alignment with the BIA, in particular with regard to adequately ensuring the redundancy of all critical components.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
		Functional	intersects with	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	5	
Article 11.6	As part of their comprehensive ICT risk management, financial entities shall:	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
Article 11.6(a)	test the ICT business continuity plans and the ICT response and recovery plans in relation to ICT systems supporting all functions at least yearly, as well as in the event of any substantive changes to ICT systems supporting critical or important functions;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
		Functional	intersects with	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
Article 11.6(b)	test the crisis communication plans established in accordance with Article 14.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
		Functional	intersects with	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	

FDE #	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 11.6 (end)	For the purposes of the first subparagraph, point (a), financial entities, other than microenterprises, shall include in the testing plans scenarios of cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities necessary to meet the obligations set out in Article 12. Financial entities shall regularly review their ICT business continuity policy and ICT response and recovery plans, taking into account the results of tests carried out in accordance with the first subparagraph and recommendations stemming from audit checks or supervisory reviews.	Functional	intersects with	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
Article 11.7	Financial entities, other than microenterprises, shall have a crisis management function, which, in the event of activation of their ICT business continuity plans or ICT response and recovery plans, shall, inter alia, set out clear procedures to manage internal and external crisis communications in accordance with Article 14.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
Article 11.8	Financial entities shall keep readily accessible records of activities before and during disruption events when their ICT business continuity plans and ICT response and recovery plans are activated.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
Article 11.9	Central securities depositories shall provide the competent authorities with copies of the results of the ICT business continuity tests, or of similar exercises.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
Article 11.10	Financial entities, other than microenterprises, shall report to the competent authorities, upon their request, an estimation of aggregated annual costs and losses caused by major ICT-related incidents.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
Article 11.11	In accordance with Article 16 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010, the ESAs, through the Joint Committee, shall by 17 July 2024develop common guidelines on the estimation of aggregated annual costs and losses referred to in paragraph 10.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
Article 12.1	For the purpose of ensuring the restoration of ICT systems and data with minimum downtime, limited disruption and loss, as part of their ICT risk management framework, financial entities shall develop and document:	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
		Functional	intersects with	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
Article 12.1(a)	backup policies and procedures specifying the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the confidentiality level of the data;	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
		Functional	intersects with	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
Article 12.1(b)	restoration and recovery procedures and methods.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
		Functional	intersects with	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
Article 12.2	Financial entities shall set up backup systems that can be activated in accordance with the backup policies and procedures, as well as restoration and recovery procedures and methods. The activation of backup systems shall not jeopardise the security of the network and information systems or the availability, authenticity, integrity or confidentiality of data. Testing of the backup procedures and restoration and recovery procedures and methods shall be undertaken periodically.	Functional	intersects with	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
		Functional	intersects with	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	5	
		Functional	intersects with	Test Restoration Using Sampling	BCD-11.5	Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.	5	
Article 12.3	When restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system. The ICT systems shall be securely protected from any unauthorised access or ICT corruption and allow for the timely restoration of services making use of data and system backups as necessary. For central counterparties, the recovery plans shall enable the recovery of all transactions at the time of disruption to allow the central counterparty to continue to operate with certainty and to complete settlement on the scheduled date. Data reporting service providers shall additionally maintain adequate resources and have back-up and restoration facilities in place in order to offer and maintain their services at all times.	Functional	intersects with	Separate Storage for Critical Information	BCD-11.2	Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up.	5	
		Functional	intersects with	Transfer to Alternate Storage Site	BCD-11.6	Mechanisms exist to transfer backup data to the alternate storage site at a rate that is capable of meeting both Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
Article 12.4	Financial entities, other than microenterprises, shall maintain redundant ICT capacities equipped with resources, capabilities and functions that are adequate to ensure business needs. Microenterprises shall assess the need to maintain such redundant ICT capacities based on their risk profile.	Functional	intersects with	Redundant Secondary System	BCD-11.7	Mechanisms exist to maintain a failover system, which is not collocated with the primary system, application and/or service, which can be activated with little-to-no loss of information or disruption to operations.	5	
		Functional	intersects with	Failover Capability	BCD-12.2	Mechanisms exist to implement real-time or near-real-time failover capability to maintain availability of critical systems, applications and/or services.	5	
Article 12.5	Central securities depositories shall maintain at least one secondary processing site endowed with adequate resources, capabilities, functions and staffing arrangements to ensure business needs. The secondary processing site shall be:	Functional	intersects with	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	5	
Article 12.5(a)	located at a geographical distance from the primary processing site to ensure that it bears a distinct risk profile and to prevent it from being affected by the event which has affected the primary site;	Functional	intersects with	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	5	
		Functional	intersects with	Separation from Primary Site	BCD-09.1	Mechanisms exist to separate the alternate processing site from the primary processing site to reduce susceptibility to similar threats.	5	
Article 12.5(b)	capable of ensuring the continuity of critical or important functions identically to the primary site, or providing the level of services necessary to ensure that the financial entity performs its critical operations within the recovery objectives;	Functional	intersects with	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	5	
Article 12.5(c)	immediately accessible to the financial entity's staff to ensure continuity of critical or important functions in the event that the primary processing site has become unavailable.	Functional	intersects with	Alternate Processing Site	BCD-09	Mechanisms exist to establish an alternate processing site that provides security measures equivalent to that of the primary site.	5	
		Functional	intersects with	Accessibility	BCD-09.2	Mechanisms exist to identify and mitigate potential accessibility problems to the alternate processing site and possible mitigation actions, in the event of an area-wide disruption or disaster.	5	

FDE #	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 12.6	In determining the recovery time and recovery point objectives for each function, financial entities shall take into account whether it is a critical or important function and the potential overall impact on market efficiency. Such time objectives shall ensure that, in extreme scenarios, the agreed service levels are met.	Functional	equal	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	10	
Article 12.7	When recovering from an ICT-related incident, financial entities shall perform necessary checks, including any multiple checks and reconciliations, in order to ensure that the highest level of data integrity is maintained. These checks shall also be performed when reconstructing data from external stakeholders, in order to ensure that all data is consistent between systems.	Functional	intersects with	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	5	
		Functional	intersects with	Test Restoration Using Sampling	BCD-11.5	Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.	5	
Article 13.1	Financial entities shall have in place capabilities and staff to gather information on vulnerabilities and cyber threats, ICT-related incidents, in particular cyber-attacks, and analyse the impact they are likely to have on their digital operational resilience.	Functional	subset of	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
		Functional	intersects with	Threat Intelligence Feeds	THR-03	Mechanisms exist to maintain situational awareness of evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
Article 13.2	Financial entities shall put in place post ICT-related incident reviews after a major ICT-related incident disrupts their core activities, analysing the causes of disruption and identifying required improvements to the ICT operations or within the ICT business continuity policy referred to in Article 11. Financial entities, other than microenterprises, shall, upon request, communicate to the competent authorities, the changes that were implemented following post ICT-related incident reviews as referred to in the first subparagraph. The post ICT-related incident reviews referred to in the first subparagraph shall determine whether the established procedures were followed and the actions taken were effective, including in relation to the following:	Functional	intersects with	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	
		Functional	intersects with	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	5	
Article 13.2(a)	the promptness in responding to security alerts and determining the impact of ICT-related incidents and their severity;	Functional	intersects with	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	
		Functional	intersects with	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	5	
Article 13.2(b)	the quality and speed of performing a forensic analysis, where deemed appropriate;	Functional	intersects with	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	
		Functional	intersects with	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	5	
Article 13.2(c)	the effectiveness of incident escalation within the financial entity;	Functional	intersects with	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	
		Functional	intersects with	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	5	
Article 13.2(d)	the effectiveness of internal and external communication.	Functional	intersects with	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	
		Functional	intersects with	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	5	
Article 13.3	Lessons derived from the digital operational resilience testing carried out in accordance with Articles 26 and 27 and from real life ICT-related incidents, in particular cyber-attacks, along with challenges faced upon the activation of ICT business continuity plans and ICT response and recovery plans, together with relevant information exchanged with counterparts and assessed during supervisory reviews, shall be duly incorporated on a continuous basis into the ICT risk assessment process. Those findings shall form the basis for appropriate reviews of relevant components of the ICT risk management framework referred to in Article 6(1).	Functional	intersects with	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	
		Functional	intersects with	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	5	
Article 13.4	Financial entities shall monitor the effectiveness of the implementation of their digital operational resilience strategy set out in Article 6(8). They shall map the evolution of ICT risk over time, analyse the frequency, types, magnitude and evolution of ICT-related incidents, in particular cyber-attacks and their patterns, with a view to understanding the level of ICT risk exposure, in particular in relation to critical or important functions, and enhance the cyber maturity and preparedness of the financial entity.	Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
Article 13.5	Senior ICT staff shall report at least yearly to the management body on the findings referred to in paragraph 3 and put forward recommendations.	Functional	subset of	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	10	
Article 13.6	Financial entities shall develop ICT security awareness programmes and digital operational resilience training as compulsory modules in their staff training schemes. Those programmes and training shall be applicable to all employees and to senior management staff, and shall have a level of complexity commensurate to the remit of their functions. Where appropriate, financial entities shall also include ICT third-party service providers in their relevant training schemes in accordance with Article 30(2), point (i).	Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
		Functional	intersects with	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
		Functional	intersects with	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: • Before authorizing access to the system or performing assigned duties; • When required by system changes; and • Annually thereafter.	5	
		Functional	intersects with	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity & data privacy awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	

FDE #	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 13.7	Financial entities, other than microenterprises, shall monitor relevant technological developments on a continuous basis, also with a view to understanding the possible impact of the deployment of such new technologies on ICT security requirements and digital operational resilience. They shall keep up-to-date with the latest ICT risk management processes, in order to effectively combat current or new forms of cyber-attacks.	Functional	subset of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
		Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to update products, including systems, software and services, to improve functionality and correct security deficiencies.	5	
Article 14.1	As part of the ICT risk management framework referred to in Article 6(1), financial entities shall have in place crisis communication plans enabling a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public, as appropriate.	Functional	intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	5	
		Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
		Functional	intersects with	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
		Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: • Internal stakeholders; • Affected clients & third-parties; and • Regulatory authorities.	5	
		Functional	intersects with	Incident Reporting Assistance	IRO-11	Mechanisms exist to provide incident response advice and assistance to users of systems for the handling and reporting of actual and potential cybersecurity & data privacy incidents.	5	
Article 14.2	As part of the ICT risk management framework, financial entities shall implement communication policies for internal staff and for external stakeholders. Communication policies for staff shall take into account the need to differentiate between staff involved in ICT risk management, in particular the staff responsible for response and recovery, and staff that needs to be informed.	Functional	intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	5	
		Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
		Functional	intersects with	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
		Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: • Internal stakeholders; • Affected clients & third-parties; and • Regulatory authorities.	5	
		Functional	intersects with	Incident Reporting Assistance	IRO-11	Mechanisms exist to provide incident response advice and assistance to users of systems for the handling and reporting of actual and potential cybersecurity & data privacy incidents.	5	
Article 14.3	At least one person in the financial entity shall be tasked with implementing the communication strategy for ICT- related incidents and fulfil the public and media function for that purpose.	Functional	intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	5	
		Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
		Functional	intersects with	Integrated Security Incident Response Team (ISIRT)	IRO-07	Mechanisms exist to establish an integrated team of cybersecurity, IT and business function representatives that are capable of addressing cybersecurity & data privacy incident response operations.	5	
		Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: • Internal stakeholders; • Affected clients & third-parties; and • Regulatory authorities.	5	
		Functional	intersects with	Incident Reporting Assistance	IRO-11	Mechanisms exist to provide incident response advice and assistance to users of systems for the handling and reporting of actual and potential cybersecurity & data privacy incidents.	5	
Article 15	The ESAs shall, through the Joint Committee, in consultation with the European Union Agency on Cybersecurity (ENISA), develop common draft regulatory technical standards in order to:	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 15(a)	specify further elements to be included in the ICT security policies, procedures, protocols and tools referred to in Article 9(2), with a view to ensuring the security of networks, enable adequate safeguards against intrusions and data misuse, preserve the availability, authenticity, integrity and confidentiality of data, including cryptographic techniques, and guarantee an accurate and prompt data transmission without major disruptions and undue delays;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 15(b)	develop further components of the controls of access management rights referred to in Article 9(4), point (c), and associated human resource policy specifying access rights, procedures for granting and revoking rights, monitoring anomalous behaviour in relation to ICT risk through appropriate indicators, including for network use patterns, hours, IT activity and unknown devices;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 15(c)	develop further the mechanisms specified in Article 10(1) enabling a prompt detection of anomalous activities and the criteria set out in Article 10(2) triggering ICT-related incident detection and response processes;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 15(d)	specify further the components of the ICT business continuity policy referred to in Article 11(1);	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 15(e)	specify further the testing of ICT business continuity plans referred to in Article 11(6) to ensure that such testing duly takes into account scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly considers the potential impact of the insolvency, or other failures, of any relevant ICT third-party service provider and, where relevant, the political risks in the respective providers' jurisdictions;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 15(f)	specify further the components of the ICT response and recovery plans referred to in Article 11(3);	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 15(g)	specifying further the content and format of the report on the review of the ICT risk management framework referred to in Article 6(5);	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 15 (end)	When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations, while duly taking into consideration any specific feature arising from the distinct nature of activities across different financial services sectors. The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024. Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first paragraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 16.1	Articles 5 to 15 of this Regulation shall not apply to small and non-interconnected investment firms, payment institutions exempted pursuant to Directive (EU) 2015/2366; institutions exempted pursuant to Directive 2013/36/EU in respect of which Member States have decided not to apply the option referred to in Article 2(4) of this Regulation; electronic money institutions exempted pursuant to Directive 2009/110/EC; and small institutions for occupational retirement provision. Without prejudice to the first subparagraph, the entities listed in the first subparagraph shall:	Functional	no relationship	N/A	N/A	N/A	N/A	

FDE #	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 16.1(a)	put in place and maintain a sound and documented ICT risk management framework that details the mechanisms and measures aimed at a quick, efficient and comprehensive management of ICT risk, including for the protection of relevant physical components and infrastructures;	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
Article 16.1(b)	continuously monitor the security and functioning of all ICT systems;	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
Article 16.1(c)	minimise the impact of ICT risk through the use of sound, resilient and updated ICT systems, protocols and tools which are appropriate to support the performance of their activities and the provision of services and adequately protect availability, authenticity, integrity and confidentiality of data in the network and information systems;	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
Article 16.1(d)	allow sources of ICT risk and anomalies in the network and information systems to be promptly identified and detected and ICT-related incidents to be swiftly handled;	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
Article 16.1(e)	identify key dependencies on ICT third-party service providers;	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
Article 16.1(f)	ensure the continuity of critical or important functions, through business continuity plans and response and recovery measures, which include, at least, back-up and restoration measures;	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
Article 16.1(g)	test, on a regular basis, the plans and measures referred to in point (f), as well as the effectiveness of the controls implemented in accordance with points (a) and (c);	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
Article 16.1(h)	implement, as appropriate, relevant operational conclusions resulting from the tests referred to in point (g) and from post-incident analysis into the ICT risk assessment process and develop, according to needs and ICT risk profile, ICT security awareness programmes and digital operational resilience training for staff and management.	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
Article 16.2	The ICT risk management framework referred to in paragraph 1, second subparagraph, point (a), shall be documented and reviewed periodically and upon the occurrence of major ICT-related incidents in compliance with supervisory instructions. It shall be continuously improved on the basis of lessons derived from implementation and monitoring. A report on the review of the ICT risk management framework shall be submitted to the competent authority upon its request.	Functional	subset of	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	10	
Article 16.3	The ESAs shall, through the Joint Committee, in consultation with the ENISA, develop common draft regulatory technical standards in order to:	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 16.2(a)	specify further the elements to be included in the ICT risk management framework referred to in paragraph 1, second subparagraph, point (a);	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 16.2(b)	specify further the elements in relation to systems, protocols and tools to minimise the impact of ICT risk referred to in paragraph 1, second subparagraph, point (c), with a view to ensuring the security of networks, enabling adequate safeguards against intrusions and data misuse and preserving the availability, authenticity, integrity and confidentiality of data;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 16.2(c)	specify further the components of the ICT business continuity plans referred to in paragraph 1, second subparagraph, point (f);	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 16.2(d)	specify further the rules on the testing of business continuity plans and ensure the effectiveness of the controls referred to in paragraph 1, second subparagraph, point (g) and ensure that such testing duly takes into account scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 16.2(e)	specify further the content and format of the report on the review of the ICT risk management framework referred to in paragraph 2.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 16.2(end)	When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations. The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024. Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 17.1	Financial entities shall define, establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents.	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
		Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
Article 17.2	Financial entities shall record all ICT-related incidents and significant cyber threats. Financial entities shall establish appropriate procedures and processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT- related incidents, to ensure that root causes are identified, documented and addressed in order to prevent the occurrence of such incidents.	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
		Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
Article 17.3	The ICT-related incident management process referred to in paragraph 1 shall:	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
Article 17.3(a)	put in place early warning indicators;	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
		Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
Article 17.3(b)	establish procedures to identify, track, log, categorise and classify ICT-related incidents according to their priority and severity and according to the criticality of the services impacted, in accordance with the criteria set out in Article 18(1);	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
		Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
Article 17.3(c)	assign roles and responsibilities that need to be activated for different ICT-related incident types and scenarios;	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
		Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
Article 17.3(d)	set out plans for communication to staff, external stakeholders and media in accordance with Article 14 and for notification to clients, for internal escalation procedures, including ICT-related customer complaints, as well as for the provision of information to financial entities that act as counterparts, as appropriate;	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
		Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
Article 17.3(e)	ensure that at least major ICT-related incidents are reported to relevant senior management and inform the management body of at least major ICT-related incidents, explaining the impact, response and additional controls to be established as a result of such ICT-related incidents;	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
		Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
Article 17.3(f)	establish ICT-related incident response procedures to mitigate impacts and ensure that services become operational and secure in a timely manner.	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	10	
		Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
Article 18.1	Financial entities shall classify ICT-related incidents and shall determine their impact based on the following criteria:	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
Article 18.1(a)	the number and/or relevance of clients or financial counterparts affected and, where applicable, the amount or number of transactions affected by the ICT-related incident, and whether the ICT-related incident has caused reputational impact;	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	

FDE #	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 18.1(b)	the duration of the ICT-related incident, including the service downtime;	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
Article 18.1(c)	the geographical spread with regard to the areas affected by the ICT-related incident, particularly if it affects more than two Member States;	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
Article 18.1(d)	the data losses that the ICT-related incident entails, in relation to availability, authenticity, integrity or confidentiality of data;	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
Article 18.1(e)	the criticality of the services affected, including the financial entity's transactions and operations;	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
Article 18.1(f)	the economic impact, in particular direct and indirect costs and losses, of the ICT-related incident in both absolute and relative terms.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
Article 18.2	Financial entities shall classify cyber threats as significant based on the criticality of the services at risk, including the financial entity's transactions and operations, number and/or relevance of clients or financial counterparts targeted and the geographical spread of the areas at risk.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover the preparation, automated detection or intake of incident reporting, analysis, containment, eradication and recovery.	5	
Article 18.3	The ESAs shall, through the Joint Committee and in consultation with the ECB and ENISA, develop common draft regulatory technical standards further specifying the following:	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 18.3(a)	the criteria set out in paragraph 1, including materiality thresholds for determining major ICT-related incidents or, as applicable, major operational or security payment-related incidents, that are subject to the reporting obligation laid down in Article 19(1);	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 18.3(b)	the criteria to be applied by competent authorities for the purpose of assessing the relevance of major ICT-related incidents or, as applicable, major operational or security payment-related incidents, to relevant competent authorities in other Member States', and the details of reports of major ICT-related incidents or, as applicable, major operational or security payment-related incidents, to be shared with other competent authorities pursuant to Article 19(6) and (7);	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 18.3(c)	the criteria set out in paragraph 2 of this Article, including high materiality thresholds for determining significant cyber threats.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 18.4	When developing the common draft regulatory technical standards referred to in paragraph 3 of this Article, the ESAs shall take into account the criteria set out in Article 4(2), as well as international standards, guidance and specifications developed and published by ENISA, including, where appropriate, specifications for other economic sectors. For the purposes of applying the criteria set out in Article 4(2), the ESAs shall duly consider the need for microenterprises and small and medium-sized enterprises to mobilise sufficient resources and capabilities to ensure that ICT-related incidents are managed swiftly. The ESAs shall submit those common draft regulatory technical standards to the Commission by 17 January 2024. Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in paragraph 3 in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 19.1	Financial entities shall report major ICT-related incidents to the relevant competent authority as referred to in Article 46 in accordance with paragraph 4 of this Article. Where a financial entity is subject to supervision by more than one national competent authority referred to in Article 46, Member States shall designate a single competent authority as the relevant competent authority responsible for carrying out the functions and duties provided for in this Article. Credit institutions classified as significant, in accordance with Article 6(4) of Regulation (EU) No 1024/2013, shall report major ICT-related incidents to the relevant national competent authority designated in accordance with Article 4 of Directive 2013/36/EU, which shall immediately transmit that report to the ECB. For the purpose of the first subparagraph, financial entities shall produce, after collecting and analysing all relevant information, the initial notification and reports referred to in paragraph 4 of this Article using the templates referred to in Article 20 and submit them to the competent authority. In the event that a technical impossibility prevents the submission of the initial notification using the template, financial entities shall notify the competent authority about it via alternative means. The initial notification and reports referred to in paragraph 4 shall include all information necessary for the competent authority to determine the significance of the major ICT-related incident and assess possible cross-border impacts. Without prejudice to the reporting pursuant to the first subparagraph by the financial entity to the relevant competent authority, Member States may additionally determine that some or all financial entities shall also provide the initial notification and each report referred to in paragraph 4 of this Article using the templates referred to in Article 20 to the competent authorities or the computer security incident response teams (CSIRTs) designated or established in accordance with Directive (EU) 2022/2555.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: • Internal stakeholders; • Affected clients & third-parties; and • Regulatory authorities.	5	
Article 19.2	Financial entities may, on a voluntary basis, notify significant cyber threats to the relevant competent authority when they deem the threat to be of relevance to the financial system, service users or clients. The relevant competent authority may provide such information to other relevant authorities referred to in paragraph 6. Credit institutions classified as significant, in accordance with Article 6(4) of Regulation (EU) No 1024/2013, may, on a voluntary basis, notify significant cyber threats to relevant national competent authority, designated in accordance with Article 4 of Directive 2013/36/EU, which shall immediately transmit the notification to the ECB. Member States may determine that those financial entities that on a voluntary basis notify in accordance with the first subparagraph may also transmit that notification to the CSIRTs designated or established in accordance with Directive (EU) 2022/2555.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: • Internal stakeholders; • Affected clients & third-parties; and • Regulatory authorities.	5	
Article 19.3	Where a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities shall, without undue delay as soon as they become aware of it, inform their clients about the major ICT-related incident and about the measures that have been taken to mitigate the adverse effects of such incident. In the case of a significant cyber threat, financial entities shall, where applicable, inform their clients that are potentially affected of any appropriate protection measures which the latter may consider taking.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: • Internal stakeholders; • Affected clients & third-parties; and • Regulatory authorities.	5	
Article 19.4	Financial entities shall, within the time limits to be laid down in accordance with Article 20, first paragraph, point (a), point (ii), submit the following to the relevant competent authority:	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: • Internal stakeholders; • Affected clients & third-parties; and • Regulatory authorities.	5	
Article 19.4(a)	an initial notification;	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: • Internal stakeholders; • Affected clients & third-parties; and • Regulatory authorities.	5	
Article 19.4(b)	an intermediate report after the initial notification referred to in point (a), as soon as the status of the original incident has changed significantly or the handling of the major ICT-related incident has changed based on new information available, followed, as appropriate, by updated notifications every time a relevant status update is available, as well as upon a specific request of the competent authority;	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: • Internal stakeholders; • Affected clients & third-parties; and • Regulatory authorities.	5	
Article 19.4(c)	a final report, when the root cause analysis has been completed, regardless of whether mitigation measures have already been implemented, and when the actual impact figures are available to replace estimates.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: • Internal stakeholders; • Affected clients & third-parties; and • Regulatory authorities.	5	

FDE #	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 19.5	Financial entities may outsource, in accordance with Union and national sectoral law, the reporting obligations under this Article to a third-party service provider. In case of such outsourcing, the financial entity remains fully responsible for the fulfilment of the incident reporting requirements.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: • Internal stakeholders; • Affected clients & third-parties; and • Regulatory authorities.	5	
Article 19.6	Upon receipt of the initial notification and of each report referred to in paragraph 4, the competent authority shall, in a timely manner, provide details of the major ICT-related incident to the following recipients based, as applicable, on their respective competences:	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 19.6(a)	EBA, ESMA or EIOPA;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 19.6(b)	the ECB, in the case of financial entities referred to in Article 2(1), points (a), (b) and (d);	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 19.6(c)	the competent authorities, single points of contact or CSIRTs designated or established in accordance with Directive (EU) 2022/2555;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 19.6(d)	the resolution authorities, as referred to in Article 3 of Directive 2014/59/EU, and the Single Resolution Board (SRB) with respect to entities referred to in Article 7(2) of Regulation (EU) No 806/2014 of the European Parliament and of the Council(37), and with respect to entities and groups referred to in Article 7(4)(b) and (5) of Regulation (EU) No 806/2014 if such details concern incidents that pose a risk to ensuring critical functions within the meaning of Article 2(1), point (35), of Directive 2014/59/EU; and	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 19.6(e)	other relevant public authorities under national law.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 19.7	Following receipt of information in accordance with paragraph 6, EBA, ESMA or EIOPA and the ECB, in consultation with ENISA and in cooperation with the relevant competent authority, shall assess whether the major ICT-related incident is relevant for competent authorities in other Member States. Following that assessment, EBA, ESMA or EIOPA shall, as soon as possible, notify relevant competent authorities in other Member States accordingly. The ECB shall notify the members of the European System of Central Banks on issues relevant to the payment system. Based on that notification, the competent authorities shall, where appropriate, take all of the necessary measures to protect the immediate stability of the financial system.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 19.8	The notification to be done by ESMA pursuant to paragraph 7 of this Article shall be without prejudice to the responsibility of the competent authority to urgently transmit the details of the major ICT-related incident to the relevant authority in the host Member State, where a central securities depository has significant cross-border activity in the host Member State, the major ICT-related incident is likely to have severe consequences for the financial markets of the host Member State and where there are cooperation arrangements among competent authorities related to the supervision of financial entities.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 23	The requirements laid down in this Chapter shall also apply to operational or security payment-related incidents and to major operational or security payment-related incidents, where they concern credit institutions, payment institutions, account information service providers, and electronic money institutions.	Functional	subset of	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	10	
Article 24.1	For the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures, financial entities, other than microenterprises, shall, taking into account the criteria set out in Article 4(2), establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework referred to in Article 6.	Functional	intersects with	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
Article 24.2	The digital operational resilience testing programme shall include a range of assessments, tests, methodologies, practices and tools to be applied in accordance with Articles 25 and 26.	Functional	intersects with	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
Article 24.3	When conducting the digital operational resilience testing programme referred to in paragraph 1 of this Article, financial entities, other than microenterprises, shall follow a risk-based approach taking into account the criteria set out in Article 4(2) duly considering the evolving landscape of ICT risk, any specific risks to which the financial entity concerned is or might be exposed, the criticality of information assets and of services provided, as well as any other factor the financial entity deems appropriate.	Functional	intersects with	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
Article 24.4	Financial entities, other than microenterprises, shall ensure that tests are undertaken by independent parties, whether internal or external. Where tests are undertaken by an internal tester, financial entities shall dedicate sufficient resources and ensure that conflicts of interest are avoided throughout the design and execution phases of the test.	Functional	intersects with	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
Article 24.5	Financial entities, other than microenterprises, shall establish procedures and policies to prioritise, classify and remedy all issues revealed throughout the performance of the tests and shall establish internal validation methodologies to ascertain that all identified weaknesses, deficiencies or gaps are fully addressed.	Functional	intersects with	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
Article 24.6	Financial entities, other than microenterprises, shall ensure, at least yearly, that appropriate tests are conducted on all ICT systems and applications supporting critical or important functions.	Functional	intersects with	Contingency Plan Testing & Exercises	BCD-04	Mechanisms exist to conduct tests and/or exercises to evaluate the contingency plan's effectiveness and the organization's readiness to execute the plan.	5	
Article 25.1	The digital operational resilience testing programme referred to in Article 24 shall provide, in accordance with the criteria set out in Article 4(2), for the execution of appropriate tests, such as vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing.	Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
		Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
Article 25.2	Central securities depositories and central counterparties shall perform vulnerability assessments before any deployment or redeployment of new or existing applications and infrastructure components, and ICT services supporting critical or important functions of the financial entity.	Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
		Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
Article 25.3	Microenterprises shall perform the tests referred to in paragraph 1 by combining a risk-based approach with a strategic planning of ICT testing, by duly considering the need to maintain a balanced approach between the scale of resources and the time to be allocated to the ICT testing provided for in this Article, on the one hand, and the urgency, type of risk, criticality of information assets and of services provided, as well as any other relevant factor, including the financial entity's ability to take calculated risks, on the other hand.	Functional	subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
		Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
Article 26.1	Financial entities, other than entities referred to in Article 16(1), first subparagraph, and other than microenterprises, which are identified in accordance with paragraph 8, third subparagraph, of this Article, shall carry out at least every 3 years advanced testing by means of TLPT. Based on the risk profile of the financial entity and taking into account operational circumstances, the competent authority may, where necessary, request the financial entity to reduce or increase this frequency.	Functional	intersects with	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	

FDE #	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 26.2	Each threat-led penetration test shall cover several or all critical or important functions of a financial entity, and shall be performed on live production systems supporting such functions. Financial entities shall identify all relevant underlying ICT systems, processes and technologies supporting critical or important functions and ICT services, including those supporting the critical or important functions which have been outsourced or contracted to ICT third-party service providers. Financial entities shall assess which critical or important functions need to be covered by the TLPT. The result of this assessment shall determine the precise scope of TLPT and shall be validated by the competent authorities.	Functional	intersects with	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	
Article 26.3	Where ICT third-party service providers are included in the scope of TLPT, the financial entity shall take the necessary measures and safeguards to ensure the participation of such ICT third-party service providers in the TLPT and shall retain at all times full responsibility for ensuring compliance with this Regulation.	Functional	intersects with	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	
Article 26.4	Without prejudice to paragraph 2, first and second subparagraphs, where the participation of an ICT third-party service provider in the TLPT, referred to in paragraph 3, is reasonably expected to have an adverse impact on the quality or security of services delivered by the ICT third-party service provider to customers that are entities falling outside the scope of this Regulation, or on the confidentiality of the data related to such services, the financial entity and the ICT third-party service provider may agree in writing that the ICT third-party service provider directly enters into contractual arrangements with an external tester, for the purpose of conducting, under the direction of one designated financial entity, a pooled TLPT involving several financial entities (pooled testing) to which the ICT third-party service provider provides ICT services. That pooled testing shall cover the relevant range of ICT services supporting critical or important functions contracted to the respective ICT third-party service provider by the financial entities. The pooled testing shall be considered TLPT carried out by the financial entities participating in the pooled testing. The number of financial entities participating in the pooled testing shall be duly calibrated taking into account the complexity and types of services involved.	Functional	intersects with	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	
Article 26.5	Financial entities shall, with the cooperation of ICT third-party service providers and other parties involved, including the testers but excluding the competent authorities, apply effective risk management controls to mitigate the risks of any potential impact on data, damage to assets, and disruption to critical or important functions, services or operations at the financial entity itself, its counterparts or to the financial sector.	Functional	intersects with	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	
Article 26.6	At the end of the testing, after reports and remediation plans have been agreed, the financial entity and, where applicable, the external testers shall provide to the authority, designated in accordance with paragraph 9 or 10, a summary of the relevant findings, the remediation plans and the documentation demonstrating that the TLPT has been conducted in accordance with the requirements.	Functional	intersects with	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	
Article 26.7	Authorities shall provide financial entities with an attestation confirming that the test was performed in accordance with the requirements as evidenced in the documentation in order to allow for mutual recognition of threat led penetration tests between competent authorities. The financial entity shall notify the relevant competent authority of the attestation, the summary of the relevant findings and the remediation plans. Without prejudice to such attestation, financial entities shall remain at all times fully responsible for the impact of the tests referred to in paragraph 4.	Functional	intersects with	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	
Article 26.8	Financial entities shall contract testers for the purposes of undertaking TLPT in accordance with Article 27. When financial entities use internal testers for the purposes of undertaking TLPT, they shall contract external testers every three tests. Credit institutions that are classified as significant in accordance with Article 6(4) of Regulation (EU) No 1024/2013, shall only use external testers in accordance with Article 27(1), points (a) to (e). Competent authorities shall identify financial entities that are required to perform TLPT taking into account the criteria set out in Article 4(2), based on an assessment of the following:	Functional	intersects with	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	
Article 26.8(a)	impact-related factors, in particular the extent to which the services provided and activities undertaken by the financial entity impact the financial sector;	Functional	intersects with	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	
Article 26.8(b)	possible financial stability concerns, including the systemic character of the financial entity at Union or national level, as applicable;	Functional	intersects with	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	
Article 26.8(c)	specific ICT risk profile, level of ICT maturity of the financial entity or technology features involved.	Functional	intersects with	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	
Article 26.9	Member States may designate a single public authority in the financial sector to be responsible for TLPT-related matters in the financial sector at national level and shall entrust it with all competences and tasks to that effect.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 26.10	In the absence of a designation in accordance with paragraph 9 of this Article, and without prejudice to the power to identify the financial entities that are required to perform TLPT, a competent authority may delegate the exercise of some or all of the tasks referred to in this Article and Article 27 to another national authority in the financial sector.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 26.11	The ESAs shall, in agreement with the ECB, develop joint draft regulatory technical standards in accordance with the TIBER-EU framework in order to specify further:	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 26.11(a)	the criteria used for the purpose of the application of paragraph 8, second subparagraph;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 26.11(b)	the requirements and standards governing the use of internal testers;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 26.11(c)	the requirements in relation to:	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 26.11(c)(i)	the scope of TLPT referred to in paragraph 2;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 26.11(c)(ii)	the testing methodology and approach to be followed for each specific phase of the testing process;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 26.11(c)(iii)	the results, closure and remediation stages of the testing;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 26.11(d)	the type of supervisory and other relevant cooperation which are needed for the implementation of TLPT, and for the facilitation of mutual recognition of that testing, in the context of financial entities that operate in more than one Member State, to allow an appropriate level of supervisory involvement and a flexible implementation to cater for specificities of financial sub-sectors or local financial markets.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 26.11 (end)	When developing those draft regulatory technical standards, the ESAs shall give due consideration to any specific feature arising from the distinct nature of activities across different financial services sectors. The ESAs shall submit those draft regulatory technical standards to the Commission by 17 July 2024. Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 27.1	Financial entities shall only use testers for the carrying out of TLPT, that:	Functional	intersects with	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5	
Article 27.1(a)	are of the highest suitability and reputability;	Functional	intersects with	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5	
Article 27.1(b)	possess technical and organisational capabilities and demonstrate specific expertise in threat intelligence, penetration testing and red team testing;	Functional	intersects with	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5	
Article 27.1(c)	are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks;	Functional	intersects with	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5	

FDE #	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 27.1(d)	provide an independent assurance, or an audit report, in relation to the sound management of risks associated with the carrying out of TLPT, including the due protection of the financial entity's confidential information and redress for the business risks of the financial entity;	Functional	intersects with	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5	
Article 27.1(e)	are duly and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence.	Functional	intersects with	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5	
Article 27.2	When using internal testers, financial entities shall ensure that, in addition to the requirements in paragraph 1, the following conditions are met:	Functional	intersects with	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5	
Article 27.2(a)	such use has been approved by the relevant competent authority or by the single public authority designated in accordance with Article 26(9) and (10);	Functional	intersects with	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5	
Article 27.2(b)	the relevant competent authority has verified that the financial entity has sufficient dedicated resources and ensured that conflicts of interest are avoided throughout the design and execution phases of the test; and	Functional	intersects with	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5	
Article 27.2(c)	the threat intelligence provider is external to the financial entity.	Functional	intersects with	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5	
Article 27.3	Financial entities shall ensure that contracts concluded with external testers require a sound management of the TLPT results and that any data processing thereof, including any generation, store, aggregation, draft, report, communication or destruction, do not create risks to the financial entity.	Functional	intersects with	Independent Penetration Agent or Team	VPM-07.1	Mechanisms exist to utilize an independent assessor or penetration team to perform penetration testing.	5	
Article 28.1	Financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework as referred to in Article 6(1), and in accordance with the following principles:	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
Article 28.1(a)	financial entities that have in place contractual arrangements for the use of ICT services to run their business operations shall, at all times, remain fully responsible for compliance with, and the discharge of, all obligations under this Regulation and applicable financial services law;	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
		Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 28.1(b)	financial entities' management of ICT third-party risk shall be implemented in light of the principle of proportionality, taking into account:	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
Article 28.1(b)(i)	the nature, scale, complexity and importance of ICT-related dependencies,	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
Article 28.1(b)(ii)	the risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers, taking into account the criticality or importance of the respective service, process or function, and the potential impact on the continuity and availability of financial services and activities, at individual and at group level.	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
Article 28.2	As part of their ICT risk management framework, financial entities, other than entities referred to in Article 16(1), first subparagraph, and other than microenterprises, shall adopt, and regularly review, a strategy on ICT third-party risk, taking into account the multi-vendor strategy referred to in Article 6(9), where applicable. The strategy on ICT third-party risk shall include a policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers and shall apply on an individual basis and, where relevant, on a sub-consolidated and consolidated basis. The management body shall, on the basis of an assessment of the overall risk profile of the financial entity and the scale and complexity of the business services, regularly review the risks identified in respect to contractual arrangements on the use of ICT services supporting critical or important functions.	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
Article 28.3	As part of their ICT risk management framework, financial entities shall maintain and update at entity level, and at sub-consolidated and consolidated levels, a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers. The contractual arrangements referred to in the first subparagraph shall be appropriately documented, distinguishing between those that cover ICT services supporting critical or important functions and those that do not. Financial entities shall report at least yearly to the competent authorities on the number of new arrangements on the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements and the ICT services and functions which are being provided. Financial entities shall make available to the competent authority, upon its request, the full register of information or, as requested, specified sections thereof, along with any information deemed necessary to enable the effective supervision of the financial entity. Financial entities shall inform the competent authority in a timely manner about any planned contractual arrangement on the use of ICT services supporting critical or important functions as well as when a function has become critical or important	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	

FDE #	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 28.3	important functions as well as when a function has become critical or important.	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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
Article 28.4	Before entering into a contractual arrangement on the use of ICT services, financial entities shall	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
Article 28.4(a)	assess whether the contractual arrangement covers the use of ICT services supporting a critical or important function;	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
		Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	5	
Article 28.4(b)	assess if supervisory conditions for contracting are met;	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
		Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	5	
Article 28.4(c)	identify and assess all relevant risks in relation to the contractual arrangement, including the possibility that such contractual arrangement may contribute to reinforcing ICT concentration risk as referred to in Article 29;	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
		Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	5	
Article 28.4(d)	undertake all due diligence on prospective ICT third-party service providers and ensure throughout the selection and assessment processes that the ICT third-party service provider is suitable;	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
		Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	5	
Article 28.4(e)	identify and assess conflicts of interest that the contractual arrangement may cause.	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
		Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	5	
Article 28.5	Financial entities may only enter into contractual arrangements with ICT third-party service providers that comply with appropriate information security standards. When those contractual arrangements concern critical or important functions, financial entities shall, prior to concluding the arrangements, take due consideration of the use, by ICT third- party service providers, of the most up-to-date and highest quality information security standards.	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
	In exercising access, inspection and audit rights over the ICT third-party service provider, financial entities shall, on the basis of a risk-based approach, pre-determine the frequency of audits and inspections as well as the areas to be audited through adhering to commonly accepted audit standards in line with any supervisory instruction on the use and incorporation of such audit standards. Where contractual arrangements concluded with ICT third-party service providers on the use of ICT services entail high technical complexity, the financial entity shall verify that auditors, whether internal or external, or a pool of auditors, possess appropriate skills and knowledge to effectively perform the relevant audits and assessments.	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	

FDE #	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 28.6		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
		Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
Article 28.7	Financial entities shall ensure that contractual arrangements on the use of ICT services may be terminated in any of the following circumstances:	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 28.7(a)	significant breach by the ICT third-party service provider of applicable laws, regulations or contractual terms;	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
		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 28.7(b)	circumstances identified throughout the monitoring of ICT third-party risk that are deemed capable of altering the performance of the functions provided through the contractual arrangement, including material changes that affect the arrangement or the situation of the ICT third-party service provider;	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
		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 28.7(c)	ICT third-party service provider's evidenced weaknesses pertaining to its overall ICT risk management and in particular in the way it ensures the availability, authenticity, integrity and, confidentiality, of data, whether personal or otherwise sensitive data, or non-personal data;	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
		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 28.7(d)	where the competent authority can no longer effectively supervise the financial entity as a result of the conditions of, or circumstances related to, the respective contractual arrangement.	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
		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 28.8	For ICT services supporting critical or important functions, financial entities shall put in place exit strategies. The exit strategies shall take into account risks that may emerge at the level of ICT third-party service providers, in particular a possible failure on their part, a deterioration of the quality of the ICT services provided, any business disruption due to inappropriate or failed provision of ICT services or any material risk arising in relation to the appropriate and continuous deployment of the respective ICT service, or the termination of contractual arrangements with ICT third-party service providers under any of the circumstances listed in paragraph 7. Financial entities shall ensure that they are able to exit contractual arrangements without:	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
		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 28.8(a)	disruption to their business activities,	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
		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 28.8(b)	limiting compliance with regulatory requirements,	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	

FDE #	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
		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 28.8(c)	detriment to the continuity and quality of services provided to clients.	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
		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/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
		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 28.8 (end)	Exit plans shall be comprehensive, documented and, in accordance with the criteria set out in Article 4(2), shall be sufficiently tested and reviewed periodically. Financial entities shall identify alternative solutions and develop transition plans enabling them to remove the contracted ICT services and the relevant data from the ICT third-party service provider and to securely and integrally transfer them to alternative providers or reincorporate them in-house. Financial entities shall have appropriate contingency measures in place to maintain business continuity in the event of the circumstances referred to in the first subparagraph.	Functional	intersects with	Alternate Sources for Continued Support	TDA-17.1	Mechanisms exist to provide in-house support or contract external providers for support with unsupported system components.	5	
Article 28.9	The ESAs shall, through the Joint Committee, develop draft implementing technical standards to establish the standard templates for the purposes of the register of information referred to in paragraph 3, including information that is common to all contractual arrangements on the use of ICT services. The ESAs shall submit those draft implementing technical standards to the Commission by 17 January 2024. Power is conferred on the Commission to adopt the implementing technical standards referred to in the first subparagraph in accordance with Article 15 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 28.10	The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to further specify the detailed content of the policy referred to in paragraph 2 in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers. When developing those draft regulatory technical standards, the ESAs shall take into account the size and the overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations. The ESAs shall submit those draft regulatory technical standards to the Commission by 17 January 2024. Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 29.1	When performing the identification and assessment of risks referred to in Article 28(4), point (c), financial entities shall also take into account whether the envisaged conclusion of a contractual arrangement in relation to ICT services supporting critical or important functions would lead to any of the following:	Functional	intersects with	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data.	5	
Article 29.1(a)	contracting an ICT third-party service provider that is not easily substitutable; or	Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	5	
Article 29.1(b)	having in place multiple contractual arrangements in relation to the provision of ICT services supporting critical or important functions with the same ICT third-party service provider or with closely connected ICT third-party service providers.	Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	5	
Article 29.1 (end)	Financial entities shall weigh the benefits and costs of alternative solutions, such as the use of different ICT third-party service providers, taking into account if and how envisaged solutions match the business needs and objectives set out in their digital resilience strateev.	Functional	intersects with	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique systems, system components or services.	5	
Article 29.2	Where the contractual arrangements on the use of ICT services supporting critical or important functions include the possibility that an ICT third-party service provider further subcontracts ICT services supporting a critical or important function to other ICT third-party service providers, financial entities shall weigh benefits and risks that may arise in connection with such subcontracting, in particular in the case of an ICT subcontractor established in a third-country. Where contractual arrangements concern ICT services supporting critical or important functions, financial entities shall duly consider the insolvency law provisions that would apply in the event of the ICT third-party service provider's bankruptcy as well as any constraint that may arise in respect to the urgent recovery of the financial entity's data. Where contractual arrangements on the use of ICT services supporting critical or important functions are concluded with an ICT third-party service provider established in a third country, financial entities shall, in addition to the considerations referred to in the second subparagraph, also consider the compliance with Union data protection rules and the effective enforcement of the law in that third country. Where the contractual arrangements on the use of ICT services supporting critical or important functions provide for subcontracting, financial entities shall assess whether and how potentially long or complex chains of subcontracting may impact their ability to fully monitor the contracted functions and the ability of the competent authority to effectively supervise the financial entity in that respect.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
		Functional	intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity & data privacy requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
Article 30.1	The rights and obligations of the financial entity and of the ICT third-party service provider shall be clearly allocated and set out in writing. The full contract shall include the service level agreements and be documented in one written document which shall be available to the parties on paper, or in a document with another downloadable, durable and accessible format.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.2	The contractual arrangements on the use of ICT services shall include at least the following elements:	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	

FDE #	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 30.2(a)	a clear and complete description of all functions and ICT services to be provided by the ICT third-party service provider, indicating whether subcontracting of an ICT service supporting a critical or important function, or material parts thereof, is permitted and, when that is the case, the conditions applying to such subcontracting;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.2(b)	the locations, namely the regions or countries, where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed, including the storage location, and the requirement for the ICT third- party service provider to notify the financial entity in advance if it envisages changing such locations;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.2(c)	provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.2(d)	provisions on ensuring access, recovery and return in an easily accessible format of personal and non-personal data processed by the financial entity in the event of the insolvency, resolution or discontinuation of the business operations of the ICT third-party service provider, or in the event of the termination of the contractual arrangements;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.2(e)	service level descriptions, including updates and revisions thereof;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.2(f)	the obligation of the ICT third-party service provider to provide assistance to the financial entity at no additional cost, or at a cost that is determined ex-ante, when an ICT incident that is related to the ICT service provided to the financial entity occurs;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.2(g)	the obligation of the ICT third-party service provider to fully cooperate with the competent authorities and the resolution authorities of the financial entity, including persons appointed by them;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.2(h)	termination rights and related minimum notice periods for the termination of the contractual arrangements, in accordance with the expectations of competent authorities and resolution authorities;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.2(i)	the conditions for the participation of ICT third-party service providers in the financial entities' ICT security awareness programmes and digital operational resilience training in accordance with Article 13(6).	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.3	The contractual arrangements on the use of ICT services supporting critical or important functions shall include, in addition to the elements referred to in paragraph 2, at least the following:	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.3(a)	full service level descriptions, including updates and revisions thereof with precise quantitative and qualitative performance targets within the agreed service levels to allow effective monitoring by the financial entity of ICT services and enable appropriate corrective actions to be taken, without undue delay, when agreed service levels are not met;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.3(b)	notice periods and reporting obligations of the ICT third-party service provider to the financial entity, including notification of any development that might have a material impact on the ICT third-party service provider's ability to effectively provide the ICT services supporting critical or important functions in line with agreed service levels;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.3(c)	requirements for the ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies that provide an appropriate level of security for the provision of services by the financial entity in line with its regulatory framework;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.3(d)	the obligation of the ICT third-party service provider to participate and fully cooperate in the financial entity's TLPT as referred to in Articles 26 and 27;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.3(e)	the right to monitor, on an ongoing basis, the ICT third-party service provider's performance, which entails the following:	Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and audit External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
Article 30.3(e)(i)	unrestricted rights of access, inspection and audit by the financial entity, or an appointed third party, and by the competent authority, and the right to take copies of relevant documentation on-site if they are critical to the operations of the ICT third-party service provider, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.3(e)(ii)	the right to agree on alternative assurance levels if other clients' rights are affected;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.3(e)(iii)	the obligation of the ICT third-party service provider to fully cooperate during the onsite inspections and audits performed by the competent authorities, the Lead Overseer, financial entity or an appointed third party; and	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.3(e)(iv)	the obligation to provide details on the scope, procedures to be followed and frequency of such inspections and audits;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.3(f)	exit strategies, in particular the establishment of a mandatory adequate transition period:	Functional	intersects with	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	
Article 30.3(f)(i)	during which the ICT third-party service provider will continue providing the respective functions, or ICT services, with a view to reducing the risk of disruption at the financial entity or to ensure its effective resolution and restructuring;	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
		Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.3 (end)	By way of derogation from point (e), the ICT third-party service provider and the financial entity that is a microenterprise may agree that the financial entity's rights of access, inspection and audit can be delegated to an independent third party, appointed by the ICT third-party service provider, and that the financial entity is able to request information and assurance on the ICT third-party service provider's performance from the third party at any time.	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
Article 30.4	When negotiating contractual arrangements, financial entities and ICT third-party service providers shall consider the use of standard contractual clauses developed by public authorities for specific services.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
Article 30.5	The ESAs shall, through the Joint Committee, develop draft regulatory technical standards to specify further the elements referred to in paragraph 2, point (a), which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions. When developing those draft regulatory technical standards, the ESAs shall take into consideration the size and overall risk profile of the financial entity, and the nature, scale and complexity of its services, activities and operations. The ESAs shall submit those draft regulatory technical standards to the Commission by 17 July 2024. Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.1	The ESAs, through the Joint Committee and upon recommendation from the Oversight Forum established pursuant to Article 32(1), shall:	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.1(a)	designate the ICT third-party service providers that are critical for financial entities, following an assessment that takes into account the criteria specified in paragraph 2;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.1(b)	appoint as Lead Overseer for each critical ICT third-party service provider the ESA that is responsible, in accordance with Regulations (EU) No 1093/2010, (EU) No 1094/2010 or (EU) No 1095/2010, for the financial entities having together the largest share of total assets out of the value of total assets of all financial entities using the services of the relevant critical ICT third-party service provider, as evidenced by the sum of the individual balance sheets of those financial entities.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.2	The designation referred to in paragraph 1, point (a), shall be based on all of the following criteria in relation to ICT services provided by the ICT third-party service provider	Functional	no relationship	N/A	N/A	N/A	N/A	

FDE #	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 31.2(a)	the systemic impact on the stability, continuity or quality of the provision of financial services in the event that the relevant ICT third-party service provider would face a large scale operational failure to provide its services, taking into account the number of financial entities and the total value of assets of financial entities to which the relevant ICT third-party service provider provides services;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.2(b)	the systemic character or importance of the financial entities that rely on the relevant ICT third-party service provider, assessed in accordance with the following parameters:	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.2(b)(i)	the number of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs) that rely on the respective ICT third-party service provider;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.2(b)(ii)	the interdependence between the G-SIIs or O-SIIs referred to in point (i) and other financial entities, including situations where the G-SIIs or O-SIIs provide financial infrastructure services to other financial entities;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.2(c)	the reliance of financial entities on the services provided by the relevant ICT third-party service provider in relation to critical or important functions of financial entities that ultimately involve the same ICT third-party service provider, irrespective of whether financial entities rely on those services directly or indirectly, through subcontracting arrangements;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.2(d)	the degree of substitutability of the ICT third-party service provider, taking into account the following parameters:	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.2(d)(i)	the lack of real alternatives, even partial, due to the limited number of ICT third-party service providers active on a specific market, or the market share of the relevant ICT third-party service provider, or the technical complexity or sophistication involved, including in relation to any proprietary technology, or the specific features of the ICT third-party service provider's organisation or activity;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.2(d)(ii)	difficulties in relation to partially or fully migrating the relevant data and workloads from the relevant ICT third- party service provider to another ICT third-party service provider, due either to significant financial costs, time or other resources that the migration process may entail, or to increased ICT risk or other operational risks to which the financial entity may be exposed through such migration.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.3	Where the ICT third-party service provider belongs to a group, the criteria referred to in paragraph 2 shall be considered in relation to the ICT services provided by the group as a whole.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.4	Critical ICT third-party service providers which are part of a group shall designate one legal person as a coordination point to ensure adequate representation and communication with the Lead Overseer.	Functional	subset of	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	10	
Article 31.5	The Lead Overseer shall notify the ICT third-party service provider of the outcome of the assessment leading to the designation referred in paragraph 1, point (a). Within 6 weeks from the date of the notification, the ICT third-party service provider may submit to the Lead Overseer a reasoned statement with any relevant information for the purposes of the assessment. The Lead Overseer shall consider the reasoned statement and may request additional information to be submitted within 30 calendar days of the receipt of such statement. After designating an ICT third-party service provider as critical, the ESAs, through the Joint Committee, shall notify the ICT third-party service provider of such designation and the starting date as from which they will effectively be subject to oversight activities. That starting date shall be no later than one month after the notification. The ICT third-party service provider shall notify the financial entities to which they provide services of their designation as critical.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.6	The Commission is empowered to adopt a delegated act in accordance with Article 57 to supplement this Regulation by specifying further the criteria referred to in paragraph 2 of this Article, by 17 July 2024.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.7	The designation referred to in paragraph 1, point (a), shall not be used until the Commission has adopted a delegated act in accordance with paragraph 6.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.8	The designation referred to in paragraph 1, point (a), shall not apply to the following:	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.8(i)	financial entities providing ICT services to other financial entities;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.8(ii)	ICT third-party service providers that are subject to oversight frameworks established for the purposes of supporting the tasks referred to in Article 127(2) of the Treaty on the Functioning of the European Union;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.8(iii)	ICT intra-group service providers;	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.8(iv)	ICT third-party service providers providing ICT services solely in one Member State to financial entities that are only active in that Member State.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.9	The ESAs, through the Joint Committee, shall establish, publish and update yearly the list of critical ICT third-party service providers at Union level.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.10	For the purposes of paragraph 1, point (a), competent authorities shall, on a yearly and aggregated basis, transmit the reports referred to in Article 28(3), third subparagraph, to the Oversight Forum established pursuant to Article 32. The Oversight Forum shall assess the ICT third-party dependencies of financial entities based on the information received from the competent authorities.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.11	The ICT third-party service providers that are not included in the list referred to in paragraph 9 may request to be designated as critical in accordance with paragraph 1, point (a). For the purpose of the first subparagraph, the ICT third-party service provider shall submit a reasoned application to EBA, ESMA or EIOPA, which, through the Joint Committee, shall decide whether to designate that ICT third-party service provider as critical in accordance with paragraph 1, point (a). The decision referred to in the second subparagraph shall be adopted and notified to the ICT third-party service provider within 6 months of receipt of the application.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 31.12	Financial entities shall only make use of the services of an ICT third-party service provider established in a third country and which has been designated as critical in accordance with paragraph 1, point (a), if the latter has established a subsidiary in the Union within the 12 months following the designation.	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
Article 31.13	The critical ICT third-party service provider referred to in paragraph 12 shall notify the Lead Overseer of any changes to the structure of the management of the subsidiary established in the Union.	Functional	no relationship	N/A	N/A	N/A	N/A	
Article 45.1	Financial entities may exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools, to the extent that such information and intelligence sharing:	Functional	intersects with	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the cybersecurity & data privacy communities to: • Facilitate ongoing cybersecurity & data privacy education and training for organizational personnel; • Maintain currency with recommended cybersecurity & data privacy practices, techniques and technologies; and • Share current cybersecurity and/or data privacy-related information including threats, vulnerabilities and incidents.	5	
		Functional	subset of	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
Article 45.1(a)	aims to enhance the digital operational resilience of financial entities, in particular through raising awareness in relation to cyber threats, limiting or impeding the cyber threats' ability to spread, supporting defence capabilities, threat detection techniques, mitigation strategies or response and recovery stages;	Functional	intersects with	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the cybersecurity & data privacy communities to: • Facilitate ongoing cybersecurity & data privacy education and training for organizational personnel; • Maintain currency with recommended cybersecurity & data privacy practices, techniques and technologies; and • Share current cybersecurity and/or data privacy-related information including threats, vulnerabilities and incidents.	5	
		Functional	subset of	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	

FDE #	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 45.1(b)	takes places within trusted communities of financial entities;	Functional	intersects with	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the cybersecurity & data privacy communities to: • Facilitate ongoing cybersecurity & data privacy education and training for organizational personnel; • Maintain currency with recommended cybersecurity & data privacy practices, techniques and technologies; and • Share current cybersecurity and/or data privacy-related information including threats, vulnerabilities and incidents.	5	
		Functional	subset of	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
Article 45.1(c)	is implemented through information-sharing arrangements that protect the potentially sensitive nature of the information shared, and that are governed by rules of conduct in full respect of business confidentiality, protection of personal data in accordance with Regulation (EU) 2016/679 and guidelines on competition policy.	Functional	intersects with	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the cybersecurity & data privacy communities to: • Facilitate ongoing cybersecurity & data privacy education and training for organizational personnel; • Maintain currency with recommended cybersecurity & data privacy practices, techniques and technologies; and • Share current cybersecurity and/or data privacy-related information including threats, vulnerabilities and incidents.	5	
		Functional	subset of	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
Article 45.2	For the purpose of paragraph 1, point (c), the information-sharing arrangements shall define the conditions for participation and, where appropriate, shall set out the details on the involvement of public authorities and the capacity in which they may be associated to the information-sharing arrangements, on the involvement of ICT third-party service providers, and on operational elements, including the use of dedicated IT platforms.	Functional	intersects with	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the cybersecurity & data privacy communities to: • Facilitate ongoing cybersecurity & data privacy education and training for organizational personnel; • Maintain currency with recommended cybersecurity & data privacy practices, techniques and technologies; and • Share current cybersecurity and/or data privacy-related information including threats, vulnerabilities and incidents.	5	
		Functional	subset of	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
Article 45.3	Financial entities shall notify competent authorities of their participation in the information-sharing arrangements referred to in paragraph 1, upon validation of their membership, or, as applicable, of the cessation of their membership, once it takes effect.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: • Internal stakeholders; • Affected clients & third-parties; and • Regulatory authorities.	5	
		Functional	subset of	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	