Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Information and Communications Technology Self-Assessment Tool

June 2026

Contents

1. Information and communications technology (ICT) Self-Assessment Tool (ICT SAT)

Background: ICT is critical to the continuous delivery of financial services, with increasing digitalisation and interconnectedness heightening exposure to cyber threats, operational disruptions, and third-party dependencies. Operational and cyber resilience are central to safeguarding consumers, maintaining market confidence, and preserving financial stability. Effective ICT risk management is therefore fundamental to the resilience and ongoing stability of Regulated Entities (REs)

Objectives: The ICT Self-Assessment Tool (ICT SAT) supports REs in evaluating their ICT risk levels and ICT control maturity through a standardised methodology aligned with Regulation (EU) 2022/2554 – the Digital Operational Resilience Act (DORA) and ICT industry best practices, enabling REs to benchmark their ICT governance and controls. Under Central Bank of Ireland's integrated, risk based supervisory approach, which focuses on material risks, completed ICT SAT's provide a structured basis for assessing digital operational resilience and broader operational risk. The Central Bank may request additional supporting evidence to verify responses.

Instructions:

- The RE should consider the proportionality principle under Article 4 of the Digital Operational Resilience Act (DORA) when completing the ICT SAT. This means that their ICT risk management framework, including policies, governance, and controls, should be proportionate to the size, nature, scale and complexity of their operations.

- The RE is kindly asked to complete ALL questions in the General Data, ICT Risk Level (RL) and ICT Risk Control (RC) tabs.

- Percentage completion rates are shown below.

- Questions are maturity level-based or closed-ended as applicable.

- Questions should be answered in a conservative manner; where an aspect of the question/response option is missing, the less mature response should be selected.

- All questionnaire responses and maturity scores should relate to current status / operational controls unless a specific time-period is required.

- When completing the strengths and weaknesses sections and noting their correlation to the relative maturity rating, for strengths, please briefly describe the ICT controls, processes, or practices that are effective, well-established, and demonstrate strong risk management or operational performance. For weaknesses, please describe any gaps relative to the control question including any ongoing or planned initiatives to address gaps that have been identified.

- Explanations should be provided to describe the implementation of controls/ measures in place and not currently in place, including reference to supporting documentation e.g. named Policies, Standards and/or Procedures to support maturity levels selected.

- Acronyms can be found in the Glossary tab.

- Please direct any questions to the Supervisory contact(s) and/or technologyrisk@centralbank.ie

Tabs	Comments	Completion
General Data	General Data contains questions designed to provide an **ICT overview** of the RE.	
ICT RL	ICT Risk Level tab encompasses questions to self-assess the firm's **overall risk level** across **five areas**.	
ICT RC	ICT Risk Control Self-Assessment comprises a series of closed questions designed to self-assess the **maturity level.**	
ICT RL Guidance ICT RC Guidance	These Guidance tabs have been created to help select the self-assessment scores within the ICT RL and ICT RC tabs.	
Glossary	A **Glossary** of key terms and abbreviations	

2. General Data

General Data		
	Entity/Contact Details	Answers
1	Name of Regulated Entity (RE)	
2	PRISM Code / Legal Entity Identifier (LEI)	< e.g. C12345 >
3	Contact person(s) / Title(s)	< e.g. Tom Murphy/Head of ICT, Firm ABC; Ann O'Brien/CISO, Group XYZ >
4	Email address(es) of contact person(s)	< e.g. Tom.Murphy@ABC.com; Walter: Ann O'Brien@groupxyz.com >
5	Telephone number of contact person(s)	< e.g. Murphy: 00353 XXXXXXXX >
6	Date of Questionnaire completion	<e.g. DD/MM/YYYY>

2.1 Details of the Regulated Entity (RE)

Details of the RE				
	Staff	Answers		Explanations
7	Number of Full Time Employees (FTE) delivering ICT services (including ICT security and ICT risk management) to the RE.	< # of RE permanent ICT FTEs >	< # of Group permanent ICT FTEs delivering ICT services to the RE >	< i.e. RE permanent ICT FTEs -> ICT employees on contracts of indefinite duration with the RE; Group ICT FTEs -> overall amount of ICT personnel on contracts of indefinite duration Group (both parent and subsidiaries/sub-entities) delivering ICT services to the RE >
8	Temporary personnel (e.g. consultants, contractors or trainees) having a fixed-term contract or provided by business partners under agreement, delivering ICT services (including ICT security and ICT risk management) to the RE.	< # of RE temporary ICT personnel >	< # of Group temporary ICT personnel delivering ICT services to the RE >	< i.e. RE temporary ICT personnel -> ICT personnel directly employed by the RE on contracts of fixed duration (e.g. temps, interns, contractors); Group Temporary ICT personnel -> overall amount of ICT personnel including Group (both parent and subsidiaries/sub-entities) on contracts of fixed duration and/or provided by business partners under agreement delivering ICT services to the RE >
9	Total number of employees (ICT and non-ICT) within the organisation.	< # of Local FTEs >	< # of Group/Total FTEs >	< i.e. Local FTEs -> all employees directly employed/contracted by the RE; Group/Total FTEs -> overall amount of personnel including Group (both parent and subsidiaries/sub-entities) >
10	Number of locations of ICT functions, business functions and data centres supporting critical and important function (CIF's) for the RE.	< # of IT function and data centre locations >	< # of business locations >	< e.g. Germany 2 (1 datacentre, 1 office premises) / UK 3 (1 datacentres, 2 offices) / Canada 2 (1 office, 1 datacentre) / Singapore 1 (1 office) A threshold can be used to report only the larger premises, answer on a best-effort basis, supplying explanations where deemed appropriate >

11	Number of ICT Risk personnel within the 2nd Line of Defence (2LOD)	< # of RE ICT Risk FTEs >	< # of Group ICT Risk FTEs >	< Please indicate the FTEs (Full Time Equivalent) working for the REs for this function. Where the personnel headcount consists of employees from outside the RE (e.g. at other Group entities), please refer to this arrangement in the explanation. >
12	Number of ICT Auditor(s) within the 3rd Line of Defence (3LOD)	< # of RE ICT Audit FTEs >	< # of Group IT Audit FTEs >	< Please indicate the FTEs (Full Time Equivalent) employed by the REs for this function. Please also detail where applicable, how many ICT Audit staff have formal ICT Audit certification(s)/qualification(s) along with respective certifying authorities. Where external auditors were utilised, please provide details (cost of contract, estimated resources employed, etc.) >

Details of the RE				
	Oversight	Answers		Explanations
13	How many Board members of the RE have ICT expertise (e.g. ICT qualification and/or ICT certification)?	< # of Board member(s) with ICT expertise >		< e.g. To qualify, a Board member would be expected to hold a recognised qualification in an ICT discipline and/or have held a position requiring significant ICT knowledge. >
14	How often is ICT, including Information Security, part of the Board agenda of the RE?	< select Frequency category >		< e.g. A standardised agenda includes ICT matters and discussed ICT matters should be officially recorded in the minutes of the Board meeting >
15	Indicate the frequency of oversight of ICT outsourced services at Senior Management / Board level.	<Frequency of KPI reviews >	< Frequency of discussion on ICT Outsourcing / Third Party ICT risks at Senior Management / Board level >	< e.g. Formal Key Performance Indicator (KPI) reviews should be documented, and remediation actions (where applicable) should have owners and timelines. Formal discussions on ICT Outsourcing risks should be officially recorded in the minutes of board meetings. >
16	Is there a formalised process that ensures that ICT strategies and governance documents (e.g. ICT policies, standards) defined at group level are tailored to comply with local regulations and operational requirements or constraints?	< Yes / No >		< Where Yes, please provide details on how this process is performed and documented here. >
17	Are you certified to any industry recognised Information Security standards?	< Yes / No >		< Please provide the name of the Information Security standard where used (e.g. NIST, ISO27k) with details of the current maturity level, tier or score as measured by the standard used. >
18	ICT Audit work performed in the last 12 months.	< # of ICT Audits in last 12 months >	< # of critical ICT findings identified in last 12 months year >	<Please provide a list of the ICT audits (either internal or external) performed in the last 12 months. <Please provide details of the most critical ICT Audit issues/findings that were closed or outstanding.>"
		< # of critical IT findings closed in last 12 months >	< # of critical ICT findings currently outstanding >	
19	Percentage of ICT audit universe **NOT** assessed by Internal Audit in the last 12 months (including outsourced ICT functions) .	< % of ICT NOT reviewed by Internal Audit in the past 12 months >	< % of ICT NOT reviewed by Internal Audit in the previous 36 months >	< When providing details of ICT functions not covered, please include outsourced ICT functions. This information may have been presented to the Audit Committee as '% of ICT Audit Universe NOT covered.' >

Details of the RE				
	IT Environment	Answers		Explanations
20	Have there been any mergers, acquisitions, carve out or other major organisational changes leading to merging or splitting of ICT landscape in the last 12 months?	< Yes / No >		< If yes, please name the mergers, acquisitions, carve out or other major organisational changes leading to merging or splitting of ICT landscape in the last 12 months. >
21	Number of critical projects with significant ICT undertaking involved planned/in progress/completed in the last 12 months.	< # of Critical Projects >		< If any, please provide name, description/purpose, start and projected end dates, current status. >
22	Past (for the last 12 months) and future / forecast ICT expenses of the RE in scope of this report (1 total figure for complete scope, in EUR)	< ICT_running_expenses_€ >	< ICT_change_expenses_€ >	< Figures can be compiled using the most recent set of accounts, or the previous financial year. Please provide appropriate commentary on source (e.g. if figures represent spends from Q3+Q4+Q1+Q2). >
		< ICT_running_expenses_forecast_€ >	< ICT_change_expenses_forecast_€ >	< Where forecasted expenses vary materially from above disbursed expenses, please outline reasons >
23	What was the total number of successful cyber-attacks (including involving outsourced service providers) in the last 12 months?	< # of successful cyber-attacks >		< Please briefly explain the type of cyber-attack (ATP, DDoS, SQL injection, etc.), the systems/processes affected and the impact (e.g. loss of availability, execution of fraudulent payments, unauthorised access, etc.). >
24	Have you observed an increasing (or decreasing) number of overall cyber-attacks on the entities in scope (both successful and unsuccessful) in the last 12 months?	< Overall Cyber Attack Activity >		< Please mention the main types of cyber-attack attempts encountered by the entity >

General Comments

3. ICT Risk Level

ICT Risk Level Questions

Unless otherwise specified, the question shall be answered in relation to the last 12 months.

3.1 ICT Security Risk

ICT Security Risk				
		Answers	Explanations	Overall ICT Risk Level Self-Assessment
1	How many external companies have access to internal systems/applications that contain sensitive information?	< # of firms e.g. 30 >	< Please list which external companies have access to your internal systems with sensitive data and purpose of access>	< Select Overall Risk Level >
2	How many data breach security incidents resulted from mobile devices and mobile / removable storage devices (such as laptops, USB sticks, smartphones, tablets, etc.) accessing the corporate network?	< # of data breach incidents e.g. 2 >	< Please briefly explain the cause of the data breaches (e.g. lost/stolen devices, unauthorised access to the corporate network, etc.).	
3a	Number of legacy (end of life: no longer supported / without extended support) ICT systems that support critical business processes (e.g. operating systems, databases systems, network systems, underlying software, excluding hardware, ATMs, mobile devices, etc)	< # of legacy systems >	< Please specify which legacy systems are going to be replaced within the next 3 years, which projects are in place aiming at migrating the legacy systems and their associated completion deadlines. >	
3b	Of which, how many critical legacy ICT systems are planned to be replaced within the next 3 years?	< # of legacy systems connected to an external	< Please specify which critical legacy systems are connected to the external network>.	
4	How many breaches of confidentiality (unauthorised access to data) were caused by security incidents (including cyber-attacks) in the past 12 months? (This should include security incidents at third party providers if such an incident led to a breach of confidentiality of information of or belonging to the RE).	< # of breaches of confidentiality e.g. 4 >	< Please briefly explain the main root causes for the breaches of confidentiality (unauthorised access to data) caused by cyber-attacks and differentiate between the security incidents at third party providers. Please indicate if some of the breaches resulted in material losses. >	

5	How many remediation actions to mitigate ICT security vulnerabilities (e.g. identified by penetration tests or vulnerability scanning) are delayed by more than 1 year?	< # remediation actions e.g. 15 >	< Please specify which remediation actions are delayed by more than 1 year. Please note that vulnerabilities of all criticality levels are in scope Please note: only distinct vulnerabilities need to be considered for this question. If one (identical, e.g. designated by a single CVE) vulnerability exists on multiple ICT assets, ICT should be considered only once.>	
6	How many critical audit, or other assessment findings related to **ICT security risk** have not been remediated for longer than 1 year?	< # findings e.g. 15 >	< Please mention the most critical and high rated findings not remediated for longer than 1 year, the root cause for the late remediation and an indication on when the remediation actions will be completed. >	

3.2 ICT Availability and Continuity Risk

ICT Availability and Continuity Risk				
		Answers	Explanations	Overall ICT Risk Level Self-Assessment
7	How many different locations or data centres (i.e. physical premises) (including ICT recovery sites and those managed by outsourced third parties) supporting/hosting business critical activities exist for the RE?	< # of locations e.g. 20 >	< This should include: - external and internal critical applications and infrastructure ICT assets, across both production and ICT recovery sites/data centres, - co located ICT assets and those mandated by regulation to be housed in country, - locations managed by outsourced third parties. Please list the locations of business-critical ICT operations/data centres and those which are outsourced. - e.g. Frankfurt - 2; London - 4; New York - 4; etc. Please clarify your definition of "critical". >	< Select Overall Risk Level >
8	How many times were the ICT continuity and/or disaster recovery plans triggered (Continuity tests and exercises/drills are not in scope)?	< # of times e.g. 5 >	< Please include reference to the date and short description of the reasons. Please list only real situations not regular testing. >	
9	How many times has the crisis incident response team been activated (excluding testing/drills)?	< # of times e.g. 5 >	< Please include reference to the date and short description of the reasons. Please list only real situations not regular testing. >	
10	How important are online and mobile presence as business distribution channels?	< i.e. 1. Not important (brochure website only), 2. Online importance increasing, 3. Already very important, 4. Critical (online and mobile only distribution channels used) >	< In answering the question, please consider how important online channels are to your business and list the critical online and mobile channels and the business services they support>	

11	What was the overall unplanned downtime (in hours, see glossary) of critical ICT systems (incl. those caused by external service providers)?	< Overall unplanned downtime in hours e.g. 9 >	< Please mention the most significant downtimes of critical ICT systems and the main root causes for these downtimes. Where unplanned downtime occurred, please list outages by system, frequency and durations (e.g. Customer verification system: 1 x 3-hour downtimes; Transaction reconciliation system: 3 x 2-hour downtimes) >	
11a	Of which, the overall unplanned downtime (in hours) that exceeded business agreements (e.g. SLA, RTO)?	< Overall unplanned downtime exceeding business agreements in hours e.g. 9 >	< Please specify the total duration of downtimes of critical ICT systems in excess of business agreements (corresponding to question #11). >	
11b	Please identify the number 1 main reason contributing to the downtime (see glossary).	< Changes (incl. software, hardware and infrastructure changes), Cyber incidents/attacks, Hardware/infrastructure failures, Capacity issues, Network issues, Database issues, Other - please explain, N/A >	< Please add explanations of the selected reason. Please select the relevant "(External party)" option in case the incident occurred at a 3rd party service provider. >	
11c	Please identify the number 2 main reason contributing to the downtime (see glossary).	< Changes (incl. software, hardware and infrastructure changes), Cyber incidents/attacks, Hardware/infrastructure failures, Capacity issues, Network issues, Database issues, Other - please explain, N/A >	< Please add explanations of the selected reason. Please select the relevant "(External party)" option in case the incident occurred at a 3rd party service provider. >	
12	How many critical audit findings, or other assessment findings related to **ICT availability and continuity risk** have not been remediated for longer than 1 year?	< # of critical findings e.g. 15 >	< Please mention the most critical and high rated findings not remediated for longer than 1 year, the root cause for the late remediation and an indication of when the remediation actions will be completed. >	

3.3 ICT Change Risk

ICT Change Risk				
		Answers	Explanations	Overall ICT Risk Level Self-Assessment
13	How would you describe the overall complexity of the ICT architecture of the entity in scope?	< 1. Low, 2. Medium, 3. High, 4. Very High >	< Please provide a reasoning for your complexity assessment (taking into account parameters such as number of networks, physical or logical platforms, applications; heterogeneity of versions used for software and hardware solutions; degree of customisation etc.). Please explain what kind of existing complexity is or might become an issue for the entity/ies in scope and what is planned to reduce this complexity. >	
14	What is the current number of critical ICT systems (such as for example operating systems, databases systems, network systems, underlying software, excluding hardware, ATMs, mobile devices, etc.) supporting critical or important functions (CIF's) for the RE?	< # of ICT systems e.g. 1000 >	< The number of systems should be provided, if possible, at the level of granularity in line with the entity's ICT asset inventory and be consistent with the answers to the items 3 and 6. >	
15	How many changes in ICT production environments hosting critical ICT systems (e.g. networks, infrastructures, critical applications and technologies supporting major business products or services) were conducted in the last 12 months?	< # of changes e.g. 400 >	< Please categorise the changes by common objectives (e.g. security updates - 200; improvement of business functionalities - 100; changes caused by new regulatory requirements; others - 100). Please clarify your definition of "critical". >	

15a	How many of the total number of changes were classified as "emergency changes"?	< # of emergency changes e.g. 200 >	< Please categorise the changes by common objectives (e.g. security updates - 200; improvement of business functionalities - 100; changes caused by new regulatory requirements; others - 100). Please clarify your definition of 'emergency change'. >	
16	How many changes in ICT production environments hosting critical ICT systems caused incidents?	< # of changes that led to issues e.g. 65 >	< Please explain common root courses for fixes needed (e.g. unexpected interdependencies between applications / wrong configuration / misalignment between test and production environment / inadequate test coverage / etc.) and related frequency >	
16a	Of the changes that encountered issues, what is the number 1 reason for the failure?	< Unexpected interdependencies between applications, Wrong configuration, Misalignment between test and production environment, Inadequate test coverage, Vendor Patches that caused issues, Other – please explain >	< Please add explanations of the selected reason. >	
16b	Of the changes that encountered issues, what is the number 2 reason for the failure?	< Unexpected interdependencies between applications, Wrong configuration, Misalignment between test and production environment, Inadequate test coverage, Vendor Patches that caused issues, Other – please explain >	< Please add explanations of the selected reason. >	

17	How many critical audit, and other assessment findings related to ICT change risk have not been remediated for longer than 1 year?	< # of critical findings e.g. 15 >	< Please mention the most critical findings not remediated for longer than 1 year, the root cause for the late remediation and an indication on when the remediation actions will be completed. Please clarify your definition of "critical". >	

3.4 ICT Third Party Risk

ICT Third Party Risk				
		Answers	Explanations	Overall ICT Risk Level Self-Assessment
18	How relevant are outsourced ICT services for critical or important functions via INTRA-group outsourcing?	<i.e. 1. Full INTRA-group outsourcing, 2. Largely INTRA-group outsourcing, 3. Partial INTRA-group outsourcing, 4. No INTRA-group outsourcing >	< Please specify which critical or important functions in ICT operations, ICT development or ICT security have been outsourced to which major INTRA-group ICT service providers (where INTRA-group are outsourcing arrangements provided by an entity belonging to the same corporate group).	
19	How relevant are outsourced ICT services for critical or important functions via EXTRA-group outsourcing?	<i.e.1. Full EXTRA-group outsourcing, 2. Largely EXTRA-group outsourcing, 3. Partial EXTRA-group outsourcing, 4. No EXTRA-group outsourcing >	< Please specify which critical or important functions in ICT operations, ICT development or ICT security have been outsourced to which major EXTRA-group ICT service providers (EXTRA-group are outsourcing arrangements provided by entities outside the corporate group). >	
20	What is the overall number of ICT outsourcing arrangements servicing critical or important functions (both INTRA-group and EXTRA-group)	< e.g. # of outsourcing arrangements >	< Please briefly describe main types of outsourcing contracts (ICT and non-ICT).>	
21	How many services for critical or important functions are delivered by cloud providers to the RE?	< e.g. 50 services >	< Please explain and provide a breakdown of services for critical or important functions delivered by ICT provides (INTRA and EXTRA-group) to the entity. > Please mention the 5 most services provided by ICT providers of the entity/ies in scope of the questionnaire. >	
22	How many critical audit, and other assessments findings related to ICT third party provider risk have not been remediated for longer than 1 year?	< e.g. 26 critical findings >	< Please mention the most critical findings not remediated for longer than 1 year, the root cause for the late remediation and an indication on when the remediation actions will be completed. Please clarify your definition of "critical". >	

3.5 ICT Data Integrity

ICT Data Integrity				
		Answers	Explanations	Overall ICT Risk Level Self-Assessment
23	What is the current number of end user-developed applications (EUDA also known as EUC - End-User-Computing) supporting critical or important functions (including Microsoft Excel spreadsheets, Microsoft Access databases and other end user-developed tools)?	< # of end-user applications e.g. 215 >	< Please name business units with the highest number of end-users developed application supporting critical or important functions (e.g. ICT - 55; Risk Management 45). >	
24	How many incidents leading to significant invalid data modifications occurred in the last 12 months?	< # of data integrity incidents e.g. 21 >	< Please briefly elaborate on the most significant invalid data modification incidents Please clarify your definition of "significant". >	
25	How many critical audit, and other assessment findings related to ICT data integrity risk have not been remediated for longer than 1 year?	< # of critical findings e.g. 15 >	< Please mention the most critical findings not remediated for longer than 1 year, the root cause for the late remediation and an indication on when the remediation actions will be completed. Please clarify your definition of "critical". >	
26	How many of the data quality issues reported internally have ICT issues as the root cause?	< # data quality issues e.g. 5 >	< Please explain the main ICT issues relevant here. >	

4. ICT Risk Control

4.1 ICT Governance and ICT Risk Management

ICT Governance and Risk Management				
1	ICT and digital operational resilience strategy	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
1.1	An ICT strategy is defined, documented, approved by the management body and aligned with the business and risk strategies (e.g. risk appetite). Senior management are involved in the definition of the RE's strategic ICT priorities. It contains an acceptable level of detail with measurable goals for the most important ICT areas, supported by concrete implementation plans and takes into account risk associated with the strategy. ICT-enabled investment programmes and projects required to achieve specific strategic business objectives are actively monitored by relevant stakeholders.	< Maturity Level >		
1.2	The RE has a Digital Operational Resilience strategy which includes methods to manage ICT risk and attain specific ICT objectives, in accordance with Article 6(8) in conjunction with Article 5(2) (d) DORA. The RE also monitors the effectiveness of the implementation of their digital operational resilience strategy and has a process in place to understand the level of ICT risk exposure, in particular in relation to critical or important functions.	< Maturity Level >		

ICT Governance and Risk Management				
2.	ICT organisation	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
2.1	The RE has established an internal governance framework for ICT risk management and accountability, in accordance with Article 5(1) & 5(2) DORA.	< Maturity Level >		
2.2	The management body of the RE holds ultimate accountability for the ICT risk management framework and digital operational resilience strategy. In accordance with Article 5(2) DORA it defines, approves, and oversees all ICT arrangements, sets ICT risk tolerance levels, establishes clear roles and responsibilities and ensures effective governance and oversight of all ICT-related incidents.	< Maturity Level >		
2.3	Members of the management body keep their ICT risk knowledge current and relevant through regular training in accordance with Article 5(4) DORA.	< Maturity Level >		

2.4	The RE includes in its human resource policy or other relevant policies all appropriate ICT security related elements in accordance with Article 19 RTS RMF.	< Maturity Level >		
2.5	The RE has identified, classified, and documented all ICT supported business functions, roles and responsibilities, and the information and ICT assets supporting those functions, including their interdependencies, it also reviews, as needed and at least yearly, the adequacy and completeness of these classifications and documentation in accordance with Article 8(1) DORA.	< Maturity Level >		
2.6	The RE has identified and mapped all information and ICT assets - including critical assets, configurations, and interdependencies - at remote sites, network resources, and hardware, and maintains inventories which are updated periodically and upon major changes, in accordance with Article 8(4) & (6) DORA.	< Maturity Level >		

2.7	In accordance with Article 8(5) DORA, the RE maintains and periodically updates a comprehensive inventory of all processes dependent on ICT third-party service providers including all identified interconnections with providers that support critical or important functions. The inventory is updated whenever any significant change occurs in the network or information system infrastructure, or in processes or procedures affecting ICT-supported business functions, information assets, or ICT assets.	< Maturity Level >		
2.8	RE conducts ICT risk assessments on a regular basis and at minimum annually for all legacy ICT systems. Additionally, ICT risk assessments are performed before connecting new technologies,	< Maturity Level >		

ICT Governance and Risk Management				
3	ICT Risk Management Framework	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
3.1	The RE has in place a documented ICT risk management framework, as part of its overall risk management system to identify, assess, and mitigate ICT risk, in accordance with Article 6 DORA & Article 3 RTS RMF. In particular the ICT risk management framework is supported by strategies, policies, procedures, ICT protocols and tools that address the following: (a) the risk tolerance for ICT risk and its approval. (b) a methodology to regularly conduct ICT risk assessments, including identifying vulnerabilities and threats that may affect the supported business functions, ICT systems and ICT assets supporting these functions and the quantitative or qualitative indicators to measure the impact and likelihood of vulnerabilities and threats. (c) a procedure to identify and document ICT risk treatment measures for ICT risks identified, to bring ICT risk within the approved risk tolerance. (d) a procedure to identify, manage and monitor any residual ICT risks still present that exceed the approved risk tolerance, including a justification for their acceptance and regular review. (e) an inventory of identified ICT risks, treatment measures	< Maturity Level >		

	and residual ICT risk. (f) provisions for the monitoring of any changes to the ICT risk and cyber threat landscape that could affect its ICT risk profile. (g) provisions for the monitoring of the effectiveness of the ICT risk treatment measures implemented and an assessment of whether the approved risk tolerance levels have been attained.			
3.2	The ICT risk management framework is reviewed at least once a year and as well as upon the occurrence of major ICT-related incidents in accordance with Article 6(5) DORA. A report on the review of the ICT risk management framework is also conducted yearly in accordance with Article 27 RTS RMF.	< Maturity Level >		
3.3	The RE, in the context of the digital operational resilience strategy referred to in Article 6(8) DORA, has defined an ICT multi-vendor strategy, showing key dependencies on ICT third-party service providers and explaining the rationale behind the procurement mix of ICT third-party service providers in accordance with Article 6(9) DORA.	< Maturity Level >		
3.4	The RE has assigned responsibility for managing and overseeing ICT risk to a control function and ensures an appropriate level of independence in order to avoid conflicts of interest in accordance with Article 6(4) DORA. REs 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, in accordance with Article 6(4) DORA.	< Maturity Level >		

3.5	The RE, on a continuous basis, identifies 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. The RE reviews on a regular basis, and at least yearly, the risk scenarios impacting it, in accordance with Article 8(2) DORA.	< Maturity Level >		

ICT Governance and Risk Management				
4	ICT Internal Audit (3LoD)	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
4.1	The ICT risk management framework is subject to internal audit on a regular basis by suitably qualified internal auditors, in accordance with Article 6 (6) DORA, with an audit plan that covers critical ICT risks (including those of outsourced activities). The audit plan reflects prior audit findings and calibrates audit frequency and scope to the entity's ICT risk profile.	< Maturity Level >		

4.2 ICT Third Party Management

ICT Third Party Risk Management				
6	Overall risk profile and Complexity	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
6.1	The RE has established an ICT third party risk management strategy in accordance with Article 28(2) DORA which is formally approved by the management body and integrated into the ICT risk management framework. The strategy includes a third-party risk management policy covering ICT services supporting critical or important functions and encompasses all the requirements set out in the Regulatory Technical Standard (RTS) ICT Third Party Policy (TPPol).	< Maturity Level >		
6.2	The RE has established and maintains a Register of Information (RoI) for all ICT third-party contractual arrangements in accordance with Article 28(3) DORA and uses the standard templates and data fields set out in ITS RoI. All contractual arrangements are appropriately documented, with clear distinctions between those supporting critical or important functions and those that do not.	< Maturity Level >		

ICT Third Party Risk Management				
7	Governance of ICT Third Party arrangements	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
7.1	In accordance with Article 28 DORA, the management body of the RE ensures that the ICT third party risk management strategy and policy are regularly reviewed, with all resulting changes approved, documented and implemented.	< Maturity Level >		
7.2	The RE's ICT third-party risk management policy is aligned with the requirements set-out RTS TPPol and provides for independent review and audits verifying compliance with legal and regulatory requirements	< Maturity Level >		
7.3	The RE's ICT third-party risk management policy in accordance with Article 8 RTS TPPol specifies that the contractual arrangements: (a) do not relieve the RE and its management body of its regulatory obligations and its responsibilities to its clients; (b) are not to prevent effective supervision of a RE and are not to contravene any supervisory restrictions on services and activities; (c) are to require that the ICT third party service providers cooperate with the competent authorities; (d) are to require that the RE, its auditors, and competent authorities have effective access to data and premises relating to the use of ICT services supporting critical or important functions.	< Maturity Level >		
7.4	For ICT assets or services operated by an ICT third-party service provider, the RE has identified and implemented the necessary requirements to maintain digital operational resilience, in accordance with the results of the data classification and ICT risk assessment, as specified in the Article 11(2)(k) RTS RMF.	< Maturity Level >		

ICT Third Party Risk Management				
8	Main phases of the life cycle for the adoption and use of contractual arrangements	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
8.1	The RE's ICT third-party risk management policy specifies the requirements, including the rules, the responsibilities and the processes, for each main phase of the lifecycle of the contractual arrangement, covering at least the following: (a) the responsibilities of the management body, including its involvement, as appropriate, in the decision-making process on the use of ICT services supporting critical or important functions provided by ICT third-party service providers; (b) the planning of contractual arrangements, including the risk assessment, the due diligence as set out in Articles 5 and 6 of the RTS TPPol and the approval process regarding new or material changes to contractual arrangements as set out in Article 8(4) of the RTS TPPol; (c) For ICT services supporting critical or important functions, the due diligence verifies the existence of risk mitigation and business continuity measures and how their functioning within the ICT third-party service provider is ensured.	< Maturity Level >		
8.2	The RE's ICT third-party risk management policy specifies the requirements, including the rules, the responsibilities and the processes, for each main phase of the lifecycle of the contractual arrangement, covering at least the following: (a) the involvement of business units, internal controls and other relevant units in respect of contractual	< Maturity Level >		

	arrangements; (b) the implementation, monitoring and management of contractual arrangements as referred to in Articles 7, 8 and 9 RTS TPPol, including at consolidated and sub-consolidated level, where applicable; (c) the documentation and record-keeping, taking into account the requirements with regard to the register of information laid down in Article 28(3) DORA; (d) the exit strategies and termination processes as set out in Article 10 RTS TPPol.			
8.3	In accordance with Article 6 RTS TPPol, the RE's ICT third-party risk management policy details which elements are to be used to assess the required level of assurance on the ICT third-party service provider's performance among: (a) audits or independent assessments performed by the RE itself or on its behalf; (b) the use of independent audit reports made on request by the ICT third-party service provider; (c) the use of audit reports made by the internal audit function of the ICT third-party service provider; (d) the use of appropriate third-party certifications; (e) the use of other relevant information available to the RE or other information provided by the ICT third-party service provider.	< Maturity Level >		
8.4	Contracts with ICT third-party providers that support critical or important ICT functions (or significant components thereof - that are eligible for subcontracting), specify: (a) the subcontractor's reporting obligations; (b) the ICT Third Party Provider must maintain continuity of ICT services across all subcontractors; (c) the RE will be notified of any material changes to subcontracting with adequate notice; (d) the RE retains termination rights.	< Maturity Level >		

ICT Third Party Risk Management				
9	Conflicts of Interest	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
9.1	In accordance with Article 6-8 of the RTS TPPol, the RE's ensures its ICT third-party risk management policy defines measures to identify, prevent, and manage actual or potential conflicts of interest with ICT third-party and intra-group service providers, provides for ongoing monitoring, and ensures that decisions on conditions, including financial conditions, for ICT services supporting critical or important functions are taken objectively.	< Maturity Level >		
9.2	Where ICT services are provided by ICT intra-group service providers, the RE's ICT third-party risk management policy specifies, that decisions on conditions, including the financial conditions, for the ICT services supporting critical or important functions are taken objectively in accordance with Article 7 RTS TPPol.	< Maturity Level >		

ICT Third Party Risk Management				
10	Contractual clauses for the use of ICT services supporting critical or important functions	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
10.1	The ICT third-party usage policy specifies that the relevant contractual arrangement shall be written and shall include all the elements set out by Article 30(2) and 30(3) of Regulation (EU) 2022/2554. The policy also includes elements regarding requirements applicable to financial entities as per Article 1(1)(a) of Regulation (EU) 2022/2554, as well as other relevant Union and national law as appropriate.	< Maturity Level >		
10.2	The RE ensures that ICT third-party contracts comply with Articles 28–30 DORA, clearly defining service scope, information assets, security and resilience requirements, subcontracting, termination, and robust access, inspection, audit, and ICT testing rights; oversight is exercised through internal audits, independent third parties, pooled audits, ICT testing (including threat led penetration testing (TLPT) where applicable), and reliance on certification reports where appropriate, while the RE retains full responsibility and accountability for compliance and operational resilience.	< Maturity Level >		
10.3	The RE's ICT third-party risk management policy ensures that it does not rely solely, over time, on third party certifications or audit reports for ICT third party service providers in accordance with Article 3 RTS TPPol.	< Maturity Level >		

10.4	The RE's ICT third-party risk management policy ensures that material changes to the relevant contractual agreement shall be formalised in a written document, dated, and signed by all parties and shall specify the renewal process for contractual arrangements in accordance with Article 4 RTS TPPol.	< Maturity Level >		

ICT Third Party Risk Management				
11	Monitoring of the contractual arrangements for the use of ICT services supporting critical or important functions and exit/termination	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
11.1	The RE's ICT third-party risk management policy, in accordance with Article 28(1), (2), & (5) DORA, ensures the continuous monitoring, assessment, and documentation of ICT third-party service providers supporting critical or important functions. This is achieved through various tools including reports, KPIs, and audits, with assessment results being used to update the entity's ICT and overall risk assessments.			
11.2	The RE ensures that its ICT third-party risk management policy, in accordance with Article 28(7) & (8) DORA defines appropriate remediation measures and contractual consequences for ICT third party service provider deficiencies or non-compliance.			
11.3	The RE has documented a realistic and periodically tested exit plan for ICT services supporting critical or important functions in accordance with Article 28 (8) DORA, taking into account severe disruption scenarios, failed service delivery, or termination of contractual arrangements.			

4.3 Information Security Management

Information Security Management				
12	Information security policies, standards, guidelines and awareness	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
12.1	The RE has established an information security policy in accordance with Article 9(4) (a) DORA which is approved by the management body and aligned to the information security objectives included in the Digital Operational Resilience strategy. The Information Security policy includes the following: (a) rules to protect the RE's information assets inline with strategy and risk appetite; (b) is applicable to all employees and third parties accessing information; (c) refers to i) ensuring the security of networks; ii) safeguards against intrusions and data misuse; iii) preserving the availability, authenticity, integrity, and confidentiality of data; (d) is communicated to all staff levels and contractors; (e) its implementation is supported by human and technical resources; (f) specifies the consequences of non-compliance by staff or by contractors.	< Maturity Level >		
12.2	The RE has put in place indicators to monitor the implementation of the ICT security policy and exceptions from it.	< Maturity Level >		

12.3	The RE has defined and implemented information security measures for the assets identified in its inventory (including software, hardware and network connections) and monitor its effectiveness to be aligned with the RE's risk tolerance and covering identified potential risks (e.g. potential fraud risk and/or possible misuses and/or abuses of confidential data).	< Maturity Level >		
12.4	All staff upon starting employment with the entity, receive mandatory training on ICT security, and Digital Operational Resilience, and periodically thereafter, in accordance with DORA Article 13(6) and RTS RMF Article 28(2)(e). Training is commensurate to the individual's role/function, seniority, or where access to data/critical systems is elevated. ICT Third Party providers are also subject to training obligations, in accordance with Article 30(2) (i) DORA.	< Maturity Level >		

Information Security Management				
13	Identity and access management (IAM)	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
13.1	The RE maintains identity and access management policies and procedures in accordance with Article 20 RTS RMF. The policies and procedures include but are not limited to: (a) unique identity corresponding to a unique user account is assigned to each staff member of the RE or staff of the ICT third-party service providers accessing the information assets and ICT assets of the RE. Records of all identity assignments are maintained, in compliance with the applicable retention requirements. (b) Lifecycle management process for identities and accounts managing the creation, change, review and update, temporary deactivation, and termination of all accounts. Where feasible and appropriate, automated solutions for the lifecycle identity management process are deployed.	< Maturity Level >		

13.2	The identity and access management policies and procedures, developed and documented in accordance with Article 21 RTS RMF, include: (a) The assignment of access rights to ICT assets based on need-to-know, need-to-use and least privilege principles, including for remote and emergency access. Need-to-know and need-to-use principles are implemented via defined job descriptions, which detail the extent of access required to perform the corresponding role/function. (b) The segregation of duties designed to prevent unjustified access to critical data/systems/premises or to prevent the allocation of combinations of access rights that may be used to circumvent controls. (c) A provision on user accountability, by limiting to the extent possible the use of generic and shared user accounts and ensuring that users are identifiable for the actions performed in the ICT systems at all times; (d) A provision on restrictions of access to ICT assets/data/systems/premises, setting out controls and tools to prevent unauthorised access. (e) account management procedures to grant, change or revoke access rights for user and generic accounts, including generic administrator accounts; (f) authentication methods; (i) the use of authentication methods commensurate to the ICT asset classification, and the overall risk profile of ICT assets; (ii) the use of strong authentication methods in accordance with leading practices and techniques for remote access to the RE's network, for privileged access, for access to ICT assets supporting critical or important functions or ICT assets that are publicly accessible. (g) physical access control measures.	< Maturity Level >		

Information Security Management				
14	Patch and vulnerability management, security reviews	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
14.1	The RE maintains patch and vulnerability management controls in accordance with Article 9(2) DORA and Article 10 RTS RMF. These controls include identification, assessment, and remediation of vulnerabilities, timely application of critical and high-risk patches, and integration with the RE's ICT risk management framework.	< Maturity Level >		
14.2	The RE conducts digital operational resilience testing and security reviews of its ICT systems, processes, and controls regularly through independent parties in accordance with Article 24 DORA. It ensures that all ICT systems supporting critical or important functions are tested at least annually. Additionally, the RE carries out advanced threat led penetration testing (TLPT) on critical and important functions at least every three years, if applicable.	< Maturity Level >		

Information Security Management				
15	Network and end-point security (incl. remote access)	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
15.1	The RE maintains network security controls in accordance Articles 13 and 14 RTS RMF. Controls include monitoring network traffic, firewalls, intrusion detection and prevention, network segmentation, and secure configuration of devices. They are integrated with the ICT risk management framework and extend to third-party providers, ensuring incidents are documented, investigated, and reported to relevant stakeholders.	< Maturity Level >		
15.2	All network security maintenance activities, including remote maintenance, are securely logged in accordance with Article 12 RTS RMF with records capturing relevant events, timestamps, and personnel.	< Maturity Level >		
15.3	The RE has implemented adequate and up-to-date protection against malware (e.g. antivirus, advanced malware prevention solutions, sandboxes) which cover the endpoints (e.g. desktops, laptops, mobile devices) as well as the servers and the gateways communicating with the external world (e.g. mail gateway and web filter) in accordance with Article 11 RTS RMF.	< Maturity Level >		

Information Security Management				
16	Security event logging and monitoring	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
16.1	The RE has implemented logging and monitoring of all network security events in accordance with Article 12(2) RTS RMF to safeguard against data misuse and intrusions. Logs record all relevant ICT events - including system access, configuration changes, and security incidents - capturing user or system identity, timestamp, affected components, and event outcomes. Logs are protected against tampering, access is controlled and auditable, and records are retained and readily available to support real-time monitoring and analysis.	< Maturity Level >		
16.2	The RE has implemented security event logging and monitoring using supporting technologies (e.g. SIEM) and dedicated teams (SOC/CERT) to detect, classify, manage, and report ICT related incidents in accordance with Article 17, 18 and 20 DORA.	< Maturity Level >		
16.3	If applicable, the RE has processes to collaborate with external entities (e.g. external computer emergency teams - CERTs, governmental authorities, telecommunication providers or ISPs, etc.) whenever required to respond to common and global cybersecurity incidents.	< Maturity Level >		

Information Security Management				
17	Physical access and environmental controls	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
17.1	The RE has implemented a physical and environmental security policy that preserves the authenticity, integrity, and availability of data including provisions for securing ICT systems and data, in accordance Article 9 DORA. The policy establishes safeguards for network and data security, protection of data in use, transit and at rest and defines physical and environmental controls (which includes securing premises, data centres, and ICT assets) in accordance with Articles 18 and 35 RTS RMF.	< Maturity Level >		

Information Security Management				
18	Data classification	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
18.1	The RE maintains a documented, approved and enforced data classification policies and procedures, in accordance with Article 8 DORA and Articles 5–6 RTS RMF that ensure ICT assets and information assets are classified by criticality and sensitivity.	< Maturity Level >		
18.2	In order to properly conduct the data classification, the RE has defined clear owners of the information assets and ensured that security measures for the detection and prevention of data loss and leakages for systems and end-point devices are identified, implemented, properly managed and continuously monitored, in accordance with Article 9 (2) DORA and Article 11 RTS RMF.	< Maturity Level >		

4.4 ICT Operations

ICT Operations				
19	ICT asset inventory and configuration management	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
19.1	Has the Applicant ensured it has an up-to-date inventory of all ICT assets/ configuration items (software and hardware including outsourced assets) with at least the following level of detail: title, description, location, state, actual configuration, ownership and criticality of all ICT assets/ configuration items as well as their relationship among each other (e.g. upstream and downstream dependencies).	< Maturity Level >		
19.2	The RE has defined and implemented an ICT Asset Management Policy and Procedure in accordance with Article 8 DORA and Article 4 and 5 RTS RMF.	< Maturity Level >		
19.3	Secure configuration baselines and hardening rules for ICT assets are defined along with measures to regularly verify that baselines are effectively deployed in accordance with Article 11(2)(b) RTS RMF.	< Maturity Level >		
19.4	Security measures are implemented to ensure that only authorised software is installed in accordance with Article 11 (2)c RTS RMF.	< Maturity Level >		

ICT Operations				
20	Availability and capacity management	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
20.1	The RE has defined and implemented a backup policy (taking into account the criticality of systems, off-site storage of backups including compliance with data classifications and media storage requirements, encryption of backups, and regular testing of backups) in accordance with Article 12 DORA.	< Maturity Level >		
20.2	The RE has defined and implemented procedures to ensure the standard operations of ICT systems, including but not limited to job scheduling processes, and logging and monitoring of ICT systems allowing the detection, analysis and correction of errors and capacity and performance management monitoring processes to ensure system resources (e.g. CPU, RAM, Hard Disk space ...) are adequate and regularly reviewed and maintained in accordance with Article 9(2) DORA and Article 8 RTS RMF.	< Maturity Level >		

ICT Operations				
21	Incident and problem management	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
21.1	The RE has defined and implemented an ICT-related incident management policy and process to detect, manage and notify ICT-related incidents in accordance with Article 17 DORA and 22 and 23 RTS RMF which include, but are not limited to: (a) 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. (b) Early warning indicators and denied roles and responsibilities for different incident types and scenarios. (c) Major incident reporting procedures are also established in accordance with Article 19 DORA; (d) A communication strategy for ICT-related incidents in accordance with Article 14(3) DORA and Article 6(8)(h) DORA).	< Maturity Level >		
21.2	The RE has a defined, documented and implemented a problem management process ensure that root causes are identified, documented and addressed to prevent reoccurrence in accordance with Article 17 DORA.	< Maturity Level >		

ICT Operations				
22	ICT change and release management	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
22.1	The RE has a defined, documented and implemented policies, procedures and controls for ICT change management in accordance with Article 9(4)(e) DORA and Article 17 RTS RMF. The policies and procedures encompass changes to software, hardware, firmware components, systems or security parameters. A risk-based approach for all ICT changes is in place to ensure all changes to ICT systems are recorded, tested, assessed, approved, implemented and verified in a controlled manner.	< Maturity Level >		
22.2	The ICT change management procedures are developed in accordance with Article 17 RTS RMF: (a) verification that ICT security requirements are met for each change; (b) mechanisms to ensure the independence of the functions that approve changes and the functions responsible for requesting and implementing those changes; (c) clearly defined roles and responsibilities (including but not limited to those of production, deployment, release management, information security and quality assurance teams, and change governance committees); (d) documentation and communication of change	< Maturity Level >		

	details; (e) fall-back procedures and responsibilities; (f) procedures to manage emergency changes; (g) procedures to document, re-evaluate, assess, and approve emergency changes after their implementation, including workarounds and patches; (h) identification of the potential impact of a change on existing ICT security measures and assessment of whether additional ICT security measures are required.			
22.3	Segregation of duties controls are clearly defined and ensure the independence of the functions that approve changes and the functions responsible for requesting and implementing those changes, in accordance with Article 17(1)(b) DORA.	< Maturity Level >		
22.4	Controls are in place to ensure that development and test environments do not contain confidential production data and test environments adequately reflect the production environment.	< Maturity Level >		

4.5 Software Acquisition, Software Development and Project Management

Software Acquisition, Software Development and Project Management				
23	ICT project management	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
23.1	A project management framework is in place for the management of all ICT projects covering as a minimum project objectives; roles and responsibilities; a project risk assessment; a project plan, timeframe and steps; key milestones and change management requirements as well as a proper analysis of information security requirements approved by a function that is independent from the development function.	< Maturity Level >		
23.2	The RE has a defined, documented and implemented an ICT project management policy in accordance with Article 15 RTS RMF, to ensure the effective management of ICT projects. The policy includes, but is not limited to the following elements: ICT project objectives; ICT project governance including roles and responsibilities; ICT project planning, timeframe and steps; identification of key stakeholders, resources and expertise required, ICT project risk assessment; relevant milestones; change management requirements, security requirements, the testing of all requirements, the approval process for deployment to production, and the identification and management of project dependencies.	< Maturity Level >		

23.3	The ICT project management policy contains governance processes to support the management and monitoring of ICT projects (e.g. project management office, an ICT steering committee, independent quality assurance process) including reporting to the management body on the progress of ICT projects (impacting CIF's) and the associated risks in accordance with Article 15 (5) RTS RMF.	< Maturity Level >		

Software Acquisition, Software Development and Project Management				
24	ICT systems acquisition, development, and maintenance	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
24.1	The RE has a defined, documented and implemented a policy to govern the acquisition, development, and maintenance of ICT systems in accordance with Article 16 RTS RMF. The policy applies to all end user computing applications supporting critical or important functions.	< Maturity Level >		
24.2	An ICT systems' acquisition, development, and maintenance procedure is documented and implemented for the testing and approval of all ICT systems prior to their use and after maintenance in accordance with Article 8 (2) (b)(v, vi and vii) & Article 16 RTS RMF. The level of testing shall be commensurate to the criticality of the business procedures and ICT assets concerned.	< Maturity Level >		

4.6 Data Quality Management

Data Quality Management				
25	Data quality management	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
25.1	The RE has defined, documented and tested data quality management procedures in accordance with Article 9(3) DORA. Data quality management procedures include ICT controls (e.g. automated input validation controls, data transfer controls, reconciliation, etc.) for the different phases of the ICT data life cycle (e.g. designing the data architecture, building the data model and/or data dictionaries, verifying data inputs, controlling data extractions, transfers and processing, including rendered data outputs, backup, etc). Data quality management procedures also apply to End User Computing (EUC).	< Maturity Level >		
25.2	Roles and responsibilities regarding data quality are clearly defined and implemented, including local data owners and a data governance function (e.g. Chief Data Office/r), responsible for: (a) issuing policies and guidelines; (b) overseeing proper implementation of the data governance and quality framework throughout the organisation; (c) ensuring the evaluation and monitoring of data quality through data quality processes; and (d) participating in relevant change management processes	< Maturity Level >		

	(such as the mergers or acquisitions of material legal entities, outsourcing of services to third parties, the launch of new products and ICT change initiatives).			
25.3	A formalised policy for management of End User Computing (EUC), for example to correctly identify, classify and protect all critical EUC assets and EUC-generated data, is in place and covers all business areas.	< Maturity Level >		

Data quality management - Please note that this refers to risk, regulatory and financial reporting data				
26	Data architecture model	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
26.1	The RE has a defined and documented data architecture, data models and data flows that include data taxonomies/ dictionaries of the main business concepts, which cover all material legal entities, business lines and material risks. The data architecture is regularly reviewed.	< Maturity Level >		

4.7 ICT Continuity Management

ICT Continuity Management				
27	Business impact analysis	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
27.1	The RE conducts a business impact analysis (BIA) of their exposures to severe business disruptions in accordance with Article 11(5) DORA. Under the BIA, the RE 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 considers 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.	< Maturity Level >		

ICT Continuity Management				
28	ICT business continuity policy and planning	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
28.1	The RE has in place an ICT business continuity policy forming an integral part of the overall business continuity policy in accordance with Article 11 DORA and Article 24 RTF RMF. The ICT business continuity policy includes the following key requirements: (a) policy objectives, scope, plans, procedures and mechanism; (b) to conduct a business impact analysis; (c) criteria to activate and deactivate all identified plans (Business continuity plans, ICT response and recovery plans and crisis communication plans) (d) governance and organisation, roles and responsibilities, and escalation procedures to implement the policy; (e) alignment of the policy to the communication policy; (f) the alignment between the ICT business continuity plans and the overall business continuity plans, concerning potential failure scenarios, including the scenarios referred to in Article 26(2) of the RTS on ICT risk management, specifying that the RE shall be able to recover the operations of its critical or important functions after disruptions within a recovery time objective and a recovery point objective; (g) the development of ICT business continuity plans for severe business disruptions, and the prioritisation of ICT business continuity actions using a risk-based approach; (h) the development, testing and review of ICT response and recovery plans, in accordance with Articles 25 and 26 of the RTS on ICT risk management; (i) the review of the effectiveness of the implemented ICT business continuity arrangements, plans,	< Maturity Level >		

	procedures and mechanisms, in accordance with Article 26 RTS RMF.			
28.2	The RE has implemented the ICT business continuity policy in accordance with Article 11(2) DORA aiming to: (a) ensure the continuity of the RE's critical or important functions; (b) respond to, and resolve, all ICT-related incidents in a way that limits damage and prioritises the resumption of activities and recovery actions; (c) activate dedicated plans that enable containment measures, processes and technologies suited to each type of ICT-related incident (d) estimate preliminary impacts, damages and losses; (e) set out communication and crisis management actions that ensure that updated information is transmitted to all relevant internal staff and external stakeholders and the competent authorities.	< Maturity Level >		
28.3	The RE maintains and periodically tests ICT business continuity plans, with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers, in accordance with Article 11 (4) DORA and Article 25 RTS RMF.	< Maturity Level >		
28.4	The RE has implemented ICT response and recovery plans which are subject to independent internal audit reviews, in accordance with Article 11(3) DORA .	< Maturity Level >		

28.5	The ICT response and recovery plans takes into account all the following, in accordance with Article 11(3) DORA and Article 26 RTS RMF: (a) the conditions prompting their activation or deactivation, and any exceptions for such activation or deactivation; (b) describe what actions are to be taken to ensure the availability, integrity, continuity, and recovery of at least ICT systems and services supporting critical or important functions of the RE; (c) designed to meet the recovery objectives of the operations of the financial entities; (d) documented and made available to the staff involved in the execution of ICT response and recovery plans and be readily accessible in case of emergency, clearly specifying roles and responsibilities; (e) provide for both short-term and long-term recovery options, including partial systems recovery; (f) include the objectives of ICT response and recovery plans and the conditions to declare a successful execution of those plans; (g) scenarios of severe business disruption such as: - cyber attacks and switch-overs between primary ICT infrastructure and redundant facilities, - quality of critical or important function deteriorates to unacceptable levels or fails, - substantial failure of ICT assets or communication infrastructure, - non-availability of critical number of staff, - impact of climate change and environment degradation, natural disasters, -insider attacks, - political and social instability, - widespread power outage.	< Maturity Level >		
28.6	The RE's ICT response and recovery plans consider alternative options, where the primary recovery measures may not be feasible in the short term because of costs, risks, logistics, or unforeseen circumstances, in accordance with Article 26(3) RTS RMF.	< Maturity Level >		

ICT Continuity Management				
29	ICT business continuity testing and review	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
29.1	At least yearly, the RE tests the ICT business continuity plans and the ICT response and recovery plans in relation to ICT systems supporting all functions, as well as in the event of any substantive changes to ICT systems supporting critical or important functions, in accordance with Article 11(6) DORA . The tests assess whether the ICT systems are able to ensure the continuity of the RE's critical or important functions through including the following: (a) test scenarios simulate potential disruptions, including an adequate set of severe but plausible scenarios including those set out in the business continuity plan, (b) testing of ICT services provided by ICT third party providers, considering scenarios linked to insolvency or failures of the ICT third-party service provider; (c) contain scenarios of cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups and redundant facilities; (d) challenges the assumptions on which business continuity plans are based; (e) contains procedures to verify the ability of the RE's staff, of ICT third-party service providers, of ICT systems, and ICT services to respond adequately to the scenarios duly taken into account in accordance with Article 26(2) of the RTS on ICT risk management framework.	< Maturity Level >		

29.2	Testing of the ICT business continuity plans is conducted and results are documented in accordance with Article 11(6) DORA and also takes into account the RE's business impact analysis and the ICT risk assessments referred to in Article 3(1)(b) RTS RMF. Any identified deficiencies resulting from that testing are analysed, addressed, and reported to the management body.	< Maturity Level >		
29.3	The RE tests the crisis communication plans established in accordance with Article 14 DORA.	< Maturity Level >		
29.4	The RE regularly reviews its ICT business continuity policy and ICT response and recovery plans, taking into account the results of tests carried out, and recommendations stemming from audit checks or supervisory reviews, in accordance with Article 11 (6) DORA.	< Maturity Level >		
29.5	The RE keeps readily accessible records of activities before and during disruption events when their ICT business continuity plans and ICT response and recovery plans are activated in accordance with Article 11(8) DORA.	< Maturity Level >		

ICT Continuity Management				
30	Crisis management and communication plans	Maturity Levels	"Strengths Please explain the maturity level selected and reference supporting documentation. "	"Weaknesses Please explain any known weaknesses relative to the control question and maturity level selected. Please also include a description of the measures taken to address the identified weaknesses."
30.1	The RE has implemented a crisis management function, which sets out clear procedures to manage internal and external crisis communications, in the event of activation of the ICT business continuity plans or ICT response and recovery plans in accordance with Article 11(7) DORA.	< Maturity Level >		
30.2	The RE has 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, in accordance with Article 14(1) DORA.	< Maturity Level >		

5. ICT Risk Level Guidance

Risk Level →	1 (Lowest exposure)	2	3	4 (Highest exposure)	COMMENT	RISK DEFINITION
Risk Category ↓	*ICT risk levels should be assessed by taking into account their inherent risks and key risk indicators reflecting on these risks as well as potential losses if these risks were to materialise.* *The assessment should also include the reflection of results of independent assessments, internal audits as well as any other relevant reviews.*					
ICT security risk	The RE would suffer no/negligible impact in the event of unauthorized access because it does not hold sensitive data on its ICT systems. Additionally, the RE has encountered no incidents, no data breaches, and no critical findings.	The RE would suffer limited impact in case of unauthorized access because it holds limited sensitive data on its ICT systems. Additionally, the RE has encountered very low number of incidents and negligible losses due to data breaches.	The RE would suffer medium impact in case of unauthorized access because of sensitive data on its ICT systems.	The RE would suffer high impact in case of unauthorized access because of sensitive data on its ICT systems.	*Data are sensitive if being stolen, altered or destroyed, it impacts business, compliance or reputation*	Any reasonably identifiable circumstance related to the use of network and information systems that, if it materializes, may compromise the security of systems, tools, processes, or the provision of services.
ICT availability and continuity risk	The RE would suffer no impact if ICT systems were to be unavailable for an extended period. Additionally, the RE has encountered no loss due to unplanned downtime of critical systems, and there are no critical findings.	The RE would suffer limited impact if ICT systems were to be unavailable for an extended period Additionally, the RE has encountered negligible losses and a negligible number of hours of unplanned downtime.	The RE would suffer medium impact if ICT systems were to be unavailable for an extended period.	The RE would suffer high impact if ICT systems were to be unavailable for an extended period.	*Extended period is to be considered relative to the business activity*	The risk that performance and availability of ICT systems and data are adversely impacted, including the inability to timely recover the RE's services, due to a failure of ICT hardware or software components; weaknesses in ICT system management; or any other event.

Risk Level →	1 (Lowest exposure)	2	3	4 (Highest exposure)	COMMENT	RISK DEFINITION
Risk Category ↓	*ICT risk levels should be assessed by taking into account their inherent risks and key risk indicators reflecting on these risks as well as potential losses if these risks were to materialise.* *The assessment should also include the reflection of results of independent assessments, internal audits as well as any other relevant reviews.*					
ICT change risk	There is a low frequency of significant changes to critical ICT systems, no bug fixes were required to fix unplanned outages caused by changes, and there are no critical findings.	There is a limited frequency of significant changes to critical ICT systems and limited bug fixes were required to fix unplanned outages caused by changes.	There is a medium frequency of significant changes to critical ICT systems.	There is a high frequency of significant changes to critical ICT systems.	*Changes on software (security patches, version upgrade, etc.) and on hardware (routers, servers, storage devices, etc.)*	The risk arising from the inability of the RE to manage ICT system changes in a timely and controlled manner, in particular for large and complex change programmes.
ICT Third Party Risk	There are no materially important third parties (e.g. intra/extra-group service providers, critical business partners, etc.) engaged with the firm providing services to support critical ICT operations.	There are a small number of materially important third parties, including intra-group, or business partners not formally classified as Outsourcing (e.g. market data providers), engaged with the firm providing services to support critical ICT operations.	There are some critical or important ICT functions / material ICT activities outsourced to service providers (including intra-group).	There are a large proportion of critical or important ICT functions / material ICT activities outsourced to service providers (including intra-group).	*Intra-group means a different legal entity to the RE.*	The risk that may arise for a RE in relation to its use of ICT services provided by ICT third-party service providers or by their subcontractors, including through outsourcing arrangements (including relevant intra-Group arrangements).

Risk Level →	1 (Lowest exposure)	2	3	4 (Highest exposure)	COMMENT	RISK DEFINITION
ICT data integrity risk	Data sources are defined to cover all critical or important functions. Additionally, the RE has not encountered any cases of invalid data modification or of incorrect supervisory reporting data submitted. There are no critical findings.	Data sources are defined but manual inputs and transfers are not fully under control. Additionally, the number of known cases of invalid data modifications and of incorrect supervisory reporting data submitted was very low.	A few data sources have been defined but sensitive data are still replicated within different bases and can be modified.	No data sources have been defined. Databases are fed with information manually.	*A data source is the main database which manages information and then is used by other applications to read data whenever needed.*	The risk that data stored and processed by ICT systems are incomplete, inaccurate or inconsistent across different ICT systems, for example as a result of weak or absent ICT controls during the different phases of the ICT data life cycle (i.e. designing the data architecture, building the data model and/or data dictionaries, verifying data inputs, controlling data extractions, transfers and processing, including rendered data outputs), impairing the ability of an RE to provide services and produce (risk) management and financial information in a correct and timely manner.

6. ICT Risk Control Guidance

Maturity Level	Criteria
1 (Best controls in place)	Controls in place are mature and well established. Controls are: - Formally documented with defined requirements, - Tested on a regular basis, - Reviewed as part of scheduled risk assessments, - Operating effectively, verified through independent testing and - Optimised to reflect best practice and automated where possible. Apart from regular maintenance, no investment is forecasted or planned in this area (i.e. no budget allocated for projects).
2	Controls are generally operating effectively and consistently across the organisation; risks are generally mitigated. Controls are: - Formally documented with defined requirements, - Tested on a regular basis, - Reviewed as part of scheduled risk assessments and - Operating effectively, verified through independent testing. Through testing and review, control improvements have been identified.
3	Some controls are in place, but they are not consistent and/or operating effectively across the entire organisation. Controls are - Formally documented with defined requirements, - Tested on a regular basis and - Reviewed as part of scheduled risk assessments A need for improvement/ investment exists, mitigation projects may be already ongoing, but the risks are not fully mitigated yet.
4	Controls are not in place and/ or risks are not effectively mitigated. Mitigation activities may have been identified but have not started yet.

7. Glossary

Term/ Acronym	Definition	Source
BIA (Business Impact Analysis)	Process of analysing activities and the effect that a business disruption might have upon them.	ISO 22301:2012
Business Continuity Plan (BCP)	Documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.	ISO 22301
CERT (Computer Emergency Response Team)	A computer emergency response team (CERT) is an expert group that handles computer security incidents.	
Critical or Important Function (CIF)	Critical or Important Function means a function where the disruption of which would materially impair the financial performance of a RE, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a RE with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law.	DORA Regulation (EU) 2022/2554
Cyber attack	A cyber-attack means a malicious ICT-related incident caused by means of an attempt perpetrated by any threat actor to destroy, expose, alter, disable, steal or gain unauthorised access to, or make unauthorised use of, an asset. A successful cyber-attack is the cyber-attack that has successfully circumvented existing defence measures.	Regulation (EU) 2022/2554 (DORA) Article 3(14)
Disaster Recovery Plan (DRP)	Documented process or set of procedures to recover and protect a business ICT infrastructure in the event of a disaster	
Downtime	The reported downtimes shall include both unavailabilities and severe performance degradations of ICT systems or services.	
End User Computing	The ability of end users to design and implement their own information system utilizing computer software products. Some examples of end-user tools are based on EXCEL or ACCESS files. Also known as EUDA - End User Developed Application.	COBIT
First Line of Defence	The first line of defence is the front-line employees who must understand their roles and responsibilities with regard to processing transactions and who must follow a systematic risk process and apply internal controls and other risk responses to treat the risks associated with those transactions.	
Legacy ICT system	An ICT system that has reached the end of its lifecycle (end-of-life), that is not suitable for upgrades or fixes, for technological or commercial reasons, or is no longer supported by its	Regulation (EU) 2022/2554

	supplier or by an ICT third-party service provider, but that is still in use and supports the functions of the RE.	(DORA) Article 3(3)
Regulated Entity (RE)	Entity regulated by the Central Bank.	
RoI	Register of Information	
Second Line of Defence	The second line of defence is the enterprise's compliance and risk functions that provide independent oversight of the risk management activities of the first line of defence.	
Security Information and event management (SIEM)	Application that provides the ability to gather relevant data from security components and audit logs to pop up alerts based on customised rules.	
Security Operations Centre (SOC)	A formally recognised function or service responsible for protecting information systems, as well as monitoring, detecting, assessing and remediating cyber threats and cyber incidents	

Abbreviation of legal texts	
DORA	Digital Operational Resilience Act
RTS	Regulatory Technical Standard
ITS	Implementing Technical Standard
RTS RMF	RTS ICT Risk Management Framework
RTS CCI	RTS Classification Criteria Incidents
RTS CTIR	RTS Content and Time limits Incident Reporting
ITS TIR	ITS Templates Incident Reporting
RTS TPPol	RTS ICT Third-Party Policy
ITS RoI	ITS Register of Information

Banc Ceannais na hÉireann
Central Bank of Ireland

Eurosystem