EUROPEAN CENTRAL BANK

BANKING SUPERVISION

IT Risk Questionnaire (ITRQ) Publication - 2026

Notice

The ECB has decided to publish, for transparency and accountability purposes, its 'Information Technology Risk Questionnaire' (ITRQ) 2026 covering the period from 1 January 2025 to 31 December 2025.

The questionnaire is designed in accordance with European Banking Authority (EBA) Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP) (EBA/GL/2017/05) as well as Regulation (EU) 2022/2554 on digital operational resilience. The ITRQ, forms an integral part of the risk assessment methodology which was developed by the European Central Bank together with the National Competent Authorities. The methodology includes thematic reviews, horizontal analyses and ICT risk topics.

The questionnaire allows for a standardised regular data collection from significant institutions under direct supervision of the European Central Bank and can be subject to updates to reflect the evolution of regulation and best practice in the domain of ICT risk.

IT Risk Questionnaire Self-Assessment

Introduction:

The supervised entity must complete the IT Risk Questionnaire (ITRQ) self-assessment, covering and including all entities owned (i.e. including owned subsidiaries) or supervised by the legal entity that received this ITRQ. Where there is a number of different legal entities (e.g. parent or subsidiary) providing ICT services, a comprehensive and holistic description of all controls is expected to be provided to the supervisor at the highest level of consolidation.

The file(s) should be submitted at the latest by 27 February 2026
(Reference period 01/01/2025 - 31/12/2025)

Tabs	Comments	Completion
Overview	This tab provides an overview of the content of the IT Risk Questionnaire (ITRQ) and a quick summary of the completion rates for those sections that need to be filled-in by the supervised entity.	
General Data	General Data contains questions designed to provide an **ICT overview** of the supervised entity.	1%
Entities in scope	Entities in scope is to describe the difference towards the prudential scope of consolidation	
ICT Risk Level Self-Assessment	ICT Risk Level (ITRL) Self-Assessment encompasses questions to self-assess the firm's **overall risk level** across several **areas**.	0%
ICT Risk Control Self-Assessment	ICT Risk Control (ITRC) Self-Assessment comprises a series of closed questions designed to self-assess the **maturity level.**	0%
Gross costs and losses	Gross costs and losses and financial recoveries in line with Regulation (EU) 2022/2554 (DORA) Article 11(10) and the EBA Joint Guidelines on estimation of aggregated annual costs and losses caused by major ICT-related incidents	
Information-sharing arrangement	Information-sharing arrangements in line with DORA Article 45	
ITRL_Guidance	These **Guidance** tabs have been created to help selecting the self-assessment scores within the ICT Risk Level (ITRL) and ICT Risk Control (ITRC) tabs.	
ITRC_Guidance	These **Guidance** tabs have been created to help selecting the self-assessment scores within the ICT Risk Level (ITRL) and ICT Risk Control (ITRC) tabs.	
Glossary	A **Glossary** of key terms has been introduced to provide explanations of some potentially ambiguous terms.	

General Data

Unless specified otherwise, the question shall be answered in relation to the reference year

	Entities in scope/contact details	Answers
1	Name(s) of supervised entity(ies) that completed the questionnaire and their respective jurisdiction(s)	< e.g. Bank ABC/Spain; Group XYZ/France >
2	JST Code (5 capital letters)	< e.g. ESABC >
3	Legal Entity Identifier code (LEI code)	< e.g. 1234ABABABABABABABAB >
4	Consolidation level	CONS
5	Contact person(s) / Title(s)	< e.g. Peter Smith/Head of IT, Bank ABC; Anna Walter/CISO, Group XYZ >
6	Email address(es) of contact person(s)	< e.g. Smith: Peter.Smith@bankABC.com; Walter: Anna.Walter@groupxyz.com >

Details of the entity in scope

	Staff	Answers 10	Answers 20	Answers 30	Explanations Please provide further details here	Has there been a material change of the definition of this item in comparison to last year's reporting?
7	Total number of employees within the group and the supervised entity (SE) as of 31.12 of reference year. If the supervised entity is the Head Quarter of the group please fill in the same figures in the group and SE columns. 7_c10: < # of Group FTEs > | 7_c20: < Of which, # of SE FTEs >	< # of Group FTEs >	< Of which, # of SE FTEs >		< i.e. Group FTEs = total number of staff members in the Group (parent and subsidiaries/sub-entities including the SE) > < i.e. SE FTEs = employees **directly on the payroll** of the supervised entity (SE) >	No
7a	Of which, number of employees (with individual permanent contract - FTEs) performing ICT related tasks (including ICT security and ICT risk management) for the supervised entity (SE) in scope, as of 31.12 of reference year. 7a_c10: < # of Group permanent ICT FTEs > | 7a_c20: < Of which, # of SE permanent ICT FTEs >	< # of Group permanent ICT FTEs >	< Of which, # of SE permanent ICT FTEs >		< i.e. permanent ICT FTEs = staff members on individual contract of indefinite duration performing ICT related tasks > < i.e. Group permanent ICT FTEs = staff under individual contract with the group (both parent and subsidiaries/sub-entities including the SE) > < i.e. SE permanent ICT FTEs = staff under individual contract directly with the SE > < The number of employees here should be equal to the sum of the employees reported under the items for the 1st, 2nd and 3rd LoD below. If there is a gap, please explain. >	No
7b	Of which, number of employees (with individual fixed-term contract - FTEs) performing ICT related tasks (including ICT security and ICT risk management) for the supervised entity (SE) in scope, as of 31.12 of reference year. 7b_c10: < # of Group non-permanent ICT FTEs > | 7b_c20: < Of which, # of SE non-permanent ICT FTEs >	< # of Group non-permanent ICT FTEs >	< Of which, # of SE non-permanent ICT FTEs >		< i.e. non-permanent ICT FTEs = employees on individual fixed-term contract performing ICT related tasks > < i.e. Group non-permanent ICT FTEs = employees under individual contract with the group (both parent and subsidiaries/sub-entities including the SE) > < i.e. SE non-permanent ICT FTEs = employees under individual contract directly with the SE >	No
8	Personnel (e.g. consultants, technical support) provided by business partners, performing ICT related tasks (including ICT security and ICT risk management) for the supervised entity (SE) in scope, as of 31.12 of reference year. 8_c10: < # of Group temporary ICT FTEs > | 8_c20: < # Of which SE temporary ICT FTEs >	< # of Group temporary ICT FTEs >	< # Of which SE temporary ICT FTEs >		< i.e. temporary ICT FTEs = personnel performing ICT related tasks for the supervised entity via non-individual contract (e.g. provided by external ICT companies, consultancy services) > < i.e. Group temporary ICT FTEs = provider(s) under contract with a group entity distinct from the SE> < i.e. SE temporary ICT FTEs = contract(s) with provider(s) signed directly by the SE >	No
9	Overall number of personnel located out of the SSM countries and performing ICT related tasks (employees of the SE, personnel provided via EXTRA-group companies) 9_c10: < Total # of SE non-SSM ICT FTEs > | 9_c20: < Of which, # of SE non-SSM permanent ICT FTEs >	< Total # of SE non-SSM ICT FTEs >	< Of which, # of SE non-SSM permanent ICT FTEs >		< Please indicate the FTEs (Full Time Equivalent) located outside the SSM countries and performing ICT related tasks for the supervised entities. The SSM countries list, as of 30/09/2021, includes: Austria, Belgium, Bulgaria, Croatia, Cyprus, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Portugal, Slovakia, Slovenia, and Spain.>	No
10	Number of locations of significant ICT functions and data centres outside the SSM countries.	< # of ICT function and data centre locations >			< e.g. Europe (outside EUR countries): 2 - London; EMEA: 1 - Singapore. The SSM countries list, as of 30/09/2021, includes: Austria, Belgium, Bulgaria, Croatia, Cyprus, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Portugal, Slovakia, Slovenia, Spain. A threshold can be used to report only the larger premises. **The key is the geographical location out of the SSM countries**. >	No
11	Is there a functional independence between 1st and 2nd Line of Defence (LoD) in the ICT risk area? 11_c20: < Name of the function / committee to which the 2 LoD in ICT area is reporting to >	< Yes / No >	< Name of the function / committee to which the 2 LoD in ICT area is reporting to >		< Please specify how the independence criteria are assured >	No
12	Number of vacant positions and percentage of staff turnover of staff performing ICT related tasks (including ICT security, ICT risk management and covering all ICT functions) of the SE 12_c10: < # of SE ICT vacancies (including ICT risk and ICT/information security) > | 12_c20: < Average period (# of months) position remained vacant at the SE> 12a_c10: < % of SE ICT staff turnover (including ICT risk and ICT/information security) > | 12a_c20: < % of total SE staff turnover >	< # of SE ICT vacancies (including ICT risk and ICT/information security) >	< Average period (# of months) position remained vacant at the SE >		< Please provide information regarding how many positions (i.e. internal permanent staff) are vacant and details for critical ICT positions, e.g. Head of ICT, Information Security Officer, etc. Please briefly elaborate on areas with the highest staff turnover rate, where staff turnover refers to the number or percentage of workers who leave the department and are replaced by new employees. Please explain how the staff turnover rate for staff performing ICT related tasks is seen compared to the overall staff turnover for the entities in scope. > < The number of vacancies here should be equal to the sum of the vacancies reported under the items for the 1st, 2nd and 3rd LoD below. If there is a gap, please explain. >	No
12a		< % of SE ICT staff turnover (including ICT risk and ICT/information security) >	< % of total SE staff turnover >			No

13 13a	Number of SE ICT personnel within the 1st Line of Defence (LoD) 13_c10: < # of SE ICT 1st LoD FTEs > | 13_c20: < # of SE ICT 1st LoD staff vacancies > 13a_c10: < % of SE ICT 1st LoD staff turnover > | 13a_c20: < Average period (# of months) position remained vacant at the SE >	< # of SE ICT 1st LoD FTEs > < % of SE ICT 1st LoD staff turnover >	< # of SE ICT 1st LoD staff vacancies > < Average period (# of months) position remained vacant at the SE >		< Please indicate the FTEs (Full Time Equivalent) working for the supervised entities for this function. Please indicate which functions are taken into account for the calculation (i.e. ICT risk, ICT operation, ICT security etc.). Please indicate and elaborate on 1LoD staff turnover, where staff turnover refers to the number or percentage of workers who leave the department and are replaced by new employees. >	No No
14 14a	Number of SE ICT Risk personnel within the 2nd Line of Defence (LoD) 14_c10: < # of SE ICT 2nd LoD FTEs > | 14_c20: < # of SE ICT 2nd LoD staff vacancies > 14a_c10: < % of SE ICT 2nd LoD staff turnover > | 14a_c20: < Average period (# of months) position remained vacant at the SE >	< # of SE ICT 2nd LoD FTEs > < % of SE ICT 2nd LoD staff turnover >	< # of SE ICT 2nd LoD staff vacancies > < Average period (# of months) position remained vacant at the SE >		< Please indicate the FTEs (Full Time Equivalent) working for the supervised entities for this function. Please indicate which functions are taken into account for the calculation (i.e. ICT risk, ICT operation, ICT security etc.). Please indicate and elaborate on ICT 2LoD staff turnover, where staff turnover refers to the number or percentage of workers who leave the department and are replaced by new employees. >	No No
15 15a	Number of SE ICT Auditor(s) within the 3rd Line of Defence (LoD) 15_c10: < # of SE ICT 3nd LoD FTEs > | 15_c20: < # of SE ICT 3nd LoD staff vacancies > 15a_c10: < % of SE ICT 3nd LoD staff turnover > | 15a_c20: < Average period (# of months) position remained vacant at the SE >	< # of SE ICT 3nd LoD FTEs > < % of SE ICT 3nd LoD staff turnover >	< # of SE ICT 3nd LoD staff vacancies > < Average period (# of months) position remained vacant at the SE >		< Please indicate the FTEs (Full Time Equivalent) employed by the supervised entities 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.). Please indicate and elaborate on ICT Audit staff turnover, where staff turnover refers to the number or percentage of workers who leave the department and are replaced by new employees. >	No No
16	Is there a legacy technology in place supporting critical or important functions, for which the relevant expertise is not easily available in the market (due to for example to the expertise not being widely taught anymore)? If answered with Yes, please add detail in the Explanation column.	< Yes / No >			< Please explain which technologies as well as critical or important functions are affected, how problematic this topic is considered and if/how it is planned to be resolved. >	No
		10	**20**	**30**		
	Financials (please refer to the Glossary for this section)	**Answers**			**Explanations**	**Has there been a material change of the definition of this item in comparison to last year's reporting?**
17 17a	Past (for the year before reference year) and future / forecast ICT expenses of the supervised entity (SE) in scope of this report (1 total figure for complete scope, in €) 17_c10: < Actual ICT running expenses for the year before the reference year in € > | 17_c20: < Actual ICT change expenses for the year before the reference year in € > 17a_c10: < ICT running expenses forecast for the year after the reference year in € > | 17a_c20: < ICT change expenses forecast for the year after the reference year in € >	< Actual ICT running expenses for the year before the reference year in € > < ICT running expenses forecast for the year after the reference year in € >	< Actual ICT change expenses for the year before the reference year in € > < ICT change expenses forecast for the year after the reference year in € >		< e.g. ICT expenses: 45,000,000€, comprising extraordinary expenses of 10,000,000€ due to a major damage in data centre A of TechbankABC caused by flooding >	No No
18	ICT expenses of the supervised entity (SE) in scope of this report (in €) for the reference year 18_c10: <ICT running expenses for the reference year in €> | 18_c20: <ICT change expenses for the reference year in €>	<ICT running expenses for the reference year in €>	<ICT change expenses for the reference year in €>		< e.g. Comprising 20,000,000€ for ICT Operations; 10,000,000€ for ICT Security Management; etc. ICT third party provider expenses are included in the ICT expenses. >	No
18a 18b	Of which, ICT expenses related to the ICT security areas of the supervised entity (SE) in the scope of this report. 18a_c10: < Overall ICT Security expenses for the reference year in € > | 18a_c20: < Overall budgeted ICT Security expenses for the year after the reference year in € > 18b_c10: < Of which, Physical ICT Security expenses for the reference year in € > | 18b_c20: < Of which, budgeted physical ICT Security expenses for the year after the reference year in € >	< Overall ICT Security expenses for the reference year in € > < Of which, Physical ICT Security expenses for the reference year in € >	< Overall budgeted ICT Security expenses for the year after the reference year in € > < Of which, budgeted physical ICT Security expenses for the year after the reference year in € >		< e.g. Comprising 20,000,000.00€ for ICT Operations; 10,000,000.00€ for ICT Security Management; etc. > < Please indicate the 5 biggest contributors to the ICT security expenses for the reference year regarding the coverage by topic (e.g. monitoring and detection, identity & access management, data leakage protection, etc.). >	No No
18c	Of which, ICT third party service provider expenses in the reference year (in €).	< Of which ICT third party provider service expenses in € >			< Please provide any comments if you deem necessary. > < Cloud expenses are to be reported in line with the definitions applied in the register of information to identify cloud services. >	No
18d	Of which, cloud expenses in the reference year (in €).	< Of which cloud expenses in € >				No
19	ICT third party service provider budget forecast for the year after the reference year (in €)	< ICT third party service provider budget forecast in € >			< e.g. The budget rises in comparison to the reference year due to the on-going project "OUT" aiming at the concentration of all ICT Operations services at techiA. >	No
20	Total amount of budget forecast (i.e. ICT + non-ICT) for the year after the reference year of the supervised entity (SE) in scope of this report (1 total figure for complete scope, in €)	< Budgeted expenses (ICT & non-ICT) for the year after the reference year in € >			< e.g. Comprising 80,000,000€ for Payroll; 30,000,000.00€ Marketing; 100,000,000€ for acquisitions; etc. >	No
20a	Total third party service provider expenses (**ICT & non-ICT**) in the reference year (in €)	< Total third party service provider expenses in € >			< Please provide any comments if you deem necessary. >	No

		10	20	30		
	Oversight	**Answers**			**Explanations**	**Has there been a material change of the definition of this item in comparison to last year's reporting?**
21	How often is ICT, including Information Security, part of the agenda of the management board and formally discussed?	< select Frequency category >			< e.g. Formally discussed ICT matters should be officially recorded in the minutes of the board meeting >	No
22	Indicate the frequency of oversight of ICT third party providers (e.g. KPI reviews, including remediation actions and associated timeframes, discussions of ICT Risks at senior management / board level) 22_c10: < Frequency of KPI reviews > | 22_c20: < Frequency of discussion on ICT third party risks at SMB level >	< Frequency of KPI reviews >	< Frequency of discussion on ICT third party risks at SMB level >		< e.g. Formal KPI reviews should be documented and remediation actions (where applicable) should have owners and timelines. Formal discussions on ICT third party risks should be officially recorded in the minutes of board meetings. >	No
23	Is there a process that ensures that ICT strategies and governance documents defined at group level are tailored to comply with local regulations and operational constraints? If answered with a Yes, please provide details on the how in the column "Explanations".	< Yes / No >			< Please provide details. >	No
24	Is the supervised entity (SE) in the scope of this report aligned to any industry recognised Information Security standards? If so, does it regularly perform a gap analysis against those standards and what is the level of alignment? 25_c10: < Yes / No alignment to IS standards > | 25_c20: < Yes / No gap analysis regularly performed > | 25_c30: < % of alignment with Information Security standards >	< Yes / No alignment to IS standards >	< Yes / No gap analysis regularly performed >	< % of alignment with Information Security standards >	< Please provide the name of the Information Security standard where used (e.g. NIST, ISO27k) with details of the current and desired maturity level, tier or score as measured by the standard used. Where alignment is not formally certified by the Information Security standard issuing authority, please outline the measurement methodology employed to assess maturity level. >	No
25	Internal ICT Audit work performed over the reference year Note that overdue must be understood as: the implementation deadline is past for open findings, and for closed findings the implementation was done after the expected deadline. Note that it covers also audit missions outsourced by the Internal Audit function to external auditor companies. 25_c10: < # of ICT Audits in reference year > 25a_c10: < Total # of ICT findings identified in reference year > | 25a_c20: < Total # of ICT findings closed in reference year > | 25a_c30: <Total # of ICT findings currently outstanding> 25b_c10: < Of which # of critical ICT findings identified in reference year > | 25b_c20: < Of which # of critical ICT findings closed in reference year > | 25b_c30: < Of which # of critical ICT findings currently outstanding> 25c_c10: < Average duration (# in months) to close critical ICT finding > 25d_c10: < Total # of overdue ICT findings > | 25d_c20: < Main type of overdue ICT findings > 25e_c10: < Of which # of overdue critical ICT findings > | 25e_c20: < Main type of overdue critical ICT findings >	< # of ICT Audits in reference year >			< Please provide details of the most critical ICT Audit issues/findings and, if any, expose reasons for excluding ICT functions from the scope of ICT Audits. Please provide a list of the ICT audits (either internal or external) performed in the last three years where the most critical findings were detected. Please specify whether the internal ICT Audit Unit is in charge of the monitoring / follow up of the remediation actions of SSM or other external ICT audits. > < Please provide the minimum length of the audit cycle (in years) for any risk related topics as well as the average length of the audit cycle (in years) for ICT risk related topics. > < Please provide details related to the overall ICT audit issues/findings and critical where indicated. Please specify how many of the current outstanding critical ICT findings are open since a year or more. >	No
25a		< Total # of ICT findings identified in reference year >	< Total # of ICT findings closed in reference year >	<Total # of ICT findings currently outstanding>		No
25b		< Of which # of critical ICT findings identified in reference year >	< Of which # of critical ICT findings closed in reference year >	< Of which # of critical ICT findings currently outstanding>		No
25c		< Average duration (# in months) to close critical ICT finding >				No
25d		< Total # of overdue ICT findings >	< Main type of overdue ICT findings >			No
25e		< Of which # of overdue critical ICT findings >	< Main type of overdue critical ICT findings >			No
26	External ICT Audit work performed over the reference year (audits of the information system performed by external auditors at the initiative of external third parties as clients, supervisors, certification agencies, etc. such as for example on-site inspections and internal model investigations) 26_c10: < Total # of external ICT findings identified in reference year > | 26_c20: < Of which # of external critical ICT findings identified in reference year >	< Total # of external ICT findings identified in reference year >	< Of which # of external critical ICT findings identified in reference year >		< Please provide details related to the external ICT audit issues/findings and critical ones. >	No

27	Percentage of ICT functions within the scope of this report NOT assessed by Internal Audit (IA) (including outsourced ICT functions) 27_c10: < % of ICT functions NOT reviewed by Internal Audit within the ref. year > | 27_c20: < % of ICT functions NOT reviewed by Internal Audit in the reference year and preceding 2 years >	< % of ICT functions NOT reviewed by Internal Audit within the ref. year >	< % of ICT functions NOT reviewed by Internal Audit in the reference year and preceding 2 years >		< Please list clearly at least top 5 functions not covered by Internal Audit. 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. >	No
27a	27a_c10: < % of ICT third party providers NOT reviewed by Internal Audit within the ref. year > | 27a_c20: < % of ICT third party providers NOT reviewed by Internal Audit in the reference year and preceding 2 years >	< % of ICT third party providers NOT reviewed by Internal Audit within the ref. year >	< % of ICT third party providers NOT reviewed by Internal Audit in the reference year and preceding 2 years >			No
		10	**20**	**30**		
	ICT Environment	**Answers**			**Explanations**	**Has there been a material change of the definition of this item in comparison to last year's reporting?**
28	Have there been any mergers, acquisitions, carve outs or other major organisational changes leading to merging or splitting of ICT landscape in the reference year for the entities in scope?	< Yes / No >			< If yes, please name the mergers, acquisitions, carve outs or other major organisational changes leading to merging or splitting of ICT landscape in the reference year. >	No
29	Number of critical projects with significant ICT undertaking involved, planned/in progress/completed in the reference year 29_c10: < Total # of projects > | 29_c20: < Related expenses in € >	< Total # of projects >	< Related expenses in € >		< Critical projects refer to the projects which the bank itself determines as the most important according to its own classification logic for projects. This logic normally considers for example a risk-based view, the criticality of ICT assets impacted and other criteria. > < If any, please provide name, description, projected and actual budget in €, start and projected end date, current status. Additionally, please indicate what is the rationale behind the projects classification (e.g. risk-based view, the criticality of ICT assets impacted and other criteria) >	No
29a	Of which, number of critical projects with impact on the ICT landscape/architecture 29a_c10: < Of which, # of projects with impact > | 29a_c20: < Related expenses in € >	< Of which, # of projects with impact >	< Related expenses in € >		< If any, please provide name, description, projected and actual budget in €, start and projected end date, current status and details on the impact on the ICT architecture. >	No
29b	Of which, number of projects related to legacy systems (replacement or mitigation) 29b_c10: < Of which, # of projects related to legacy systems > | 29b_c20: < Related expenses in € >	< Of which, # of projects related to legacy systems >	< Related expenses in € >		< If any, please provide name, description, projected and actual budget in €, start and projected end date, current status, goals (replacement or mitigation of legacy systems). >	No
30	What was the total number of successful cyber-attacks (including those aiming at third party providers) in the reference year? 30_c10: < # of successful cyber attacks >	< # 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.). >	No
30a	30a_c10: < Average time for detection (all type of cyber-attacks - in hours) > | 30a_c20: < Average time for recovery (all type of cyber-attacks - in hours) >	< Average time for detection (all type of cyber-attacks - in hours) >	< Average time for recovery (all type of cyber-attacks - in hours) >			No
30b	30b_c10: < Average time for detection (cyber-attacks excluding DDOS - in hours) > | 30b_c20: < Average time for recovery (cyber-attacks excluding DDOS - in hours) >	< Average time for detection (cyber-attacks excluding DDOS - in hours) >	< Average time for recovery (cyber-attacks excluding DDOS - in hours) >			No
31	Have you observed an increasing (or decreasing) number of overall cyber-attacks on the entities in scope (both successful and unsuccessful) in the reference year?	< Significantly increasing, Slightly increasing, Relatively stable, Slightly decreasing, Significantly decreasing >			< Please also include some key numbers (e.g. cyber alerts or cyber-attacks), based on which you have come to your conclusion on the trend, including a short explanation. Note: please take into consideration the internal / procedural factors like e.g. the expansion or enhancement of your detection capabilities may impact the number of attack attempts that your institution is able to see. If at all feasible, please try to offset these internal factors, to indicate the trends in the external threat environment of your institution. >	No
32	What was the total amount of direct and indirect costs (e.g. losses, resulting penalties or fees, expenses for response and recovery activities, staff hours, involvement of external experts) due to successful cyber-attacks including those aiming at outsourced service providers in the reference year (in €)? 32_c10: < Overall amount of losses in € > | 32_c20: < Of which, amount of losses due to cyber-attacks aiming at outsourced providers in € >	< Overall amount of losses in € >	< Of which, amount of losses due to cyber-attacks aiming at outsourced providers in € >		< Please mention the main loss drivers of the total amount of losses due to successful cyber-attacks. Please briefly explain the main root causes for the incidents caused by cyber-attacks. Please ensure that all type of direct and indirect costs are covered in your calculation. >	No
33	Does the supervised entity (SE) in the scope of this report have insurance contracts covering cyber-risk? 33_c20: < Maximum insurance coverage per year in € > | 33_c30: < Deductible amount per claim in €>	< Yes / No >	< Maximum insurance coverage per year in € >	< Deductible amount per claim in €>	< Please briefly explain the insurance contracts in place and main type of ICT risk covered and/or not covered. Please briefly explain calculation of the direct and indirect costs. >	No
34	Does the supervised entity (SE) in the scope of this report have projects or researches in the area of "innovation": big data, usage of Artificial Intelligence, moving core functions to cloud, implement blockchain technologies, PSD2, crypto currencies or fin-tech companies? 34_c20: < Number of on-going projects related to "innovation" > | 34_c30: < Of which number of projects to be implemented in the next 24 months >	< Yes / No >	< # of on-going projects related to "innovation" >	< Of which # of projects to be implemented in the next 24 months >	< Please specify and provide any further details on the main key areas and related projects, investments done >	No
35	What is your main current operating model for ICT project management?	< Waterfall, Agile, DevOps, Other - please explain >			< Please specify and provide any further details such as the standards that your current operating model is based on >	No
36	What was the total amount of losses (e.g. customer compensation, lost business) caused by unavailability or poor quality of services of ICT third party providers in the reference year (in €)?	< Overall amount of losses in € >			< Please name which service providers caused the biggest amount of losses and briefly describe the root cause. >	No

37	How many critical audit, on-site inspection and internal model investigation findings related to ICT third party provider risk have not been remediated for longer than 1 year? (as of 31.12 of reference year)	< # of 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". >	No
38	When was the last time the ICT risk management framework was reviewed in line with Article 6(5) of Regulation (EU) 2022/2554? What was the trigger for that review? Which function conducted the review? 38_c10: < Date of the latest review, e.g. 04/11/2025 > 38_c30: < Function conducting the review >	< Date of the latest review, e.g. 04/11/2025 >	< Periodical review, Major ICT-related incident, Conclusions from digital operational resilience testing/audit process >	< Function conducting the review >	< Please add additional explanations if the trigger of the review was not a periodical review. >	No

	General comments	

Entity name (In case the entity is in-/excluded in/from the scope of this questionnaire in comparison to the group structure reported under COREP C06.02)	**LEI Code (if available)**	**Consolidation level**	**Excluded/Included**	**Explanation for the inclusion/exclusion and other relevant comments**

	Questions to the ICT Risk Level Unless specified otherwise, the question shall be answered in relation to the reference year	Answers	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	Has there been a material change of the definition of this item in comparison to last year's reporting?	Overall ICT Risk Level Self-Assessment
	ICT security risk				
1	How many external companies (all that are different from the entity/ies in scope) have access to internal systems/applications that contain sensitive information classified as either confidential or strictly confidential (as of 31.12 of reference year)?	< # of firms e.g. 30 >	< Please specify which external companies typically have the most frequent access to your internal systems or data and why. Please specify the number of individuals belonging to external companies that have any kind of access to internal systems or data. >	No	< 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 during the reference year?	< # 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.). Please note that not only the highest criticality incidents are in scope of this question, but all criticality levels. >	No	
3	Number of critical legacy ICT systems (such as for example operating systems, databases systems, network systems, underlying software, excluding hardware, ATMs, mobile devices, etc. as of 31.12 of reference year).	< # of legacy systems >	< The number of systems should be provided, if possible, at the level of granularity in line with the entity's ICT asset inventory (see glossary) and be consistent with the answers to the items 6 and 22. Please specify which business critical processes are dependent on legacy systems and to which extent. Please indicate which system is legacy (if there are too many indicate the total number); which projects are in place aiming at migrating the legacy systems and their associated completion deadlines. >	No	
3a	Of which, how many critical legacy ICT systems are planned to be replaced within next year (i.e. a concrete project for the legacy system replacement which is at least planned and approved)?	< # of legacy systems to be replaced >	< Please specify which legacy systems are going to be replaced within next year, which projects are in place aiming at migrating the legacy systems and their associated completion deadlines. >	No	
3b	Of which, for how many critical legacy ICT systems, which are not planned to be replaced next year, there are migration plan(s) in place as to replace them in maximum 3 years horizon?	< # of legacy systems with migration plan >	< Please specify in case there are no migration plans. Please specify type of legacy and how many there are per type in %. >	No	
4	How many critical ICT systems are expected to become legacy within the next year?	< # of systems expected to become legacy >	< Please specify which systems are going to become legacy. In case there are too many such systems, please specify those with the highest level of criticality. >	No	
5	How many critical business applications are relying on one or several of the critical legacy ICT systems reported above?	< # of applications relying on an legacy system >	< Please explain if there is a mitigation plan in place regarding the risk related to these applications. >	No	
6	Number of legacy ICT systems (such as for example operating systems, databases systems, network systems, underlying software, excluding hardware, ATMs, mobile devices, etc.) that are connected to any external networks (as of 31.12 of reference year). The number of systems should be provided 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 22.	< # of legacy systems connected to an external system >	< Please specify which legacy systems are connected to the external network. Please specify the type of legacy and how many they are per type in %. >	No	
7	How many breaches of confidentiality (unauthorised access to data) were caused by security incidents (including cyber-attacks) in the reference year? 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 supervised entity.	< # 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. In case there is a gap between internally reported significant incidents caused by cyber-attacks and the ones submitted to the supervisor, please explain. Please indicate if some of the breaches resulted in material losses. >	No	
7a	For the breaches of confidentiality caused by security incidents, please specify average detection time, in hours (i.e. time to detect the incident).	< average detection time in hours e.g. 4 >	< Please specify the shortest and longest detection times of security incidents and how they were detected. >	No	
7b	For the breaches of confidentiality caused by security incidents, please specify average recovery (resolution) time, in hours.	< average recovery time in hours e.g. 4 >	< Please specify the shortest and longest recovery times of security incidents and how many FTEs were involved. >	No	
8	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 or planned for longer than 1 year? (as of 31.12 of reference year). 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.	< # remediation actions e.g. 15 >	< Please specify which remediation actions are delayed by more than 1 year and initiatives planned to remediate ICT security vulnerabilities lasting longer than 1 year. Please note that vulnerabilities of all criticality levels are in scope.>	No	
8a	Of which, the number of remediation actions to mitigate ICT security vulnerabilities (e.g. identified by penetration tests or vulnerability scanning) that are overdue (as of 31.12 of reference year).	< # overdue remediation actions e.g. 5 >	< Please specify which remediation actions are overdue, the main reasons for the delay and initiatives planned to remediate it. >	No	
9	How many critical audit, on-site inspection and internal model investigation findings related to ICT security risk have not been remediated for longer than 1 year (as of 31.12 of reference year)?	< # 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. >	No	
	ICT availability and continuity risk				
10	How many different locations or data centres (namely physical addresses) (including ICT recovery sites) supporting/hosting business critical activities exist for the entity/ies in scope? (as of 31.12 of reference year) This should include external and internal critical applications and infrastructure ICT assets, across both production and ICT recovery sites/data centres, as well as co located ICT assets and those mandated by regulation to be housed in country?	< # of locations e.g. 20 >	< Please describe what you consider as a business critical ICT operations/data centre. Please list the locations of business critical ICT operations/data centres. - e.g. Frankfurt - 2; London - 4; New York - 4; etc. Please clarify your definition of "critical". >	No	< Select Overall Risk Level >
10a	Of which: the number of outsourced data centres supporting/hosting critical or important functions?	< # of outsourced data centres e.g. 10 >	< Please specify the number of data centres supporting/hosting critical activities which are operated by third party service providers. >	No	
11	How many times were the ICT continuity and disaster recovery (DRP) plans triggered during the reference year (Continuity tests and exercises 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. >	No	
12	How many times has the crisis incident response team been activated (excluding exercises) during the reference year?	< # 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. >	No	
13	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) >	< Please mention key indicators used by the entity/ies in scope showing the importance of online or mobile presence and their development in the reference year compared to the previous year (e.g. number of granted loans via the online banking compared to total number of granted loans). >	No	
14	Does the entity in scope provide critical ICT services to other institutions where a disruption could potentially impact the financial sector either at domestic or international level (e.g. major service provider for national payment system) (as of 31.12 of reference year)?	< Yes / No >	< Please list the critical ICT services offered to other institutions and your approximate market share in this service in SSM countries. >	No	
15	What was the overall unplanned downtime (in hours, see glossary) of critical ICT systems in the reference year (incl. those caused by external service providers)? Where applicable, please provide breakdown of any outage by system, frequency and duration(s) in the Explanation section?	< 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 provide itemisation of outages by system, frequency and durations (e.g. Customer verification system: 1 x 3 hour downtimes; Transaction reconciliation system: 3 x 2 hour downtimes) >	No	
15a	Of which, the overall unplanned downtime (in hours, see glossary) 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 #15a). >	No	
15b	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. >	No	
15c	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. >	No	

	Questions to the ICT Risk Level Unless specified otherwise, the question shall be answered in relation to the reference year	Answers	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	Has there been a material change of the definition of this item in comparison to last year's reporting?	Overall ICT Risk Level Self-Assessment
15d	Please identify the number 3 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. >	No	
16	What was the overall number of unplanned downtimes (see glossary) of critical ICT systems in the reference year (incl. those caused by external service providers)?	< # of unplanned downtimes >	< Please report the number of downtimes of critical ICT systems (corresponding to question above regarding the overall unplanned downtime in hours). >	No	
16a	Of which, the number of unplanned downtimes (see glossary) that exceeded business agreements (e.g. SLA, RTO).	< # of unplanned downtimes exceeding business agreements >	< Please specify how many downtimes exceeded business agreements. Please specify the main root causes for these downtimes. >	No	
17	What was the amount of losses (direct and indirect) due to the disruption of critical ICT systems (incl. those caused by external service providers) and with material impact to customers in the reference year (in €)?	< Overall amount of losses in € >	< Please mention the major loss drivers. Please use the definition of "Critical System" outlined in the Glossary tab or clarify your definition of "critical". >	No	
18	What was the overall unplanned downtime (in hours, see glossary) of material customer service due to ICT disruptions in the reference year? Where applicable, please provide a breakdown of any outage by service, frequency and duration(s) in the Explanation section.	< Overall unplanned downtime in hours e.g. 17 >	< Please mention the most significant customer service disruptions and the main root causes for these disruptions. Please clarify your definition of "significant". Where unplanned downtime occurred, please provide itemisation of disruptions by service, frequency and duration (e.g. ATM network system: 2 x 3 hour downtimes; Online banking website: 1 x 5 hour downtime; Call centre availability: 1 x 2 hour, 1 x 4 hour downtimes) >	No	
19	What was the overall number of unplanned downtimes (see glossary) of material customer service due to ICT disruptions in the reference year?	< # of unplanned downtimes >	< Please specify the number of unplanned downtimes of material customer services (corresponding to question #17). >	No	
20	How many critical audit, on-site inspection and internal model investigation findings related to ICT availability and continuity risk have not been remediated for longer than 1 year (as of 31.12 of reference 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 of when the remediation actions will be completed. >	No	
	ICT change risk				
21	How would you describe the overall complexity of the ICT architecture of the entity in scope (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.)? (as of 31.12 of reference year)	< 1. Low, 2. Medium, 3. High, 4. Very High >	< Please provide a reasoning for your complexity assessment. 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. >	No	
22	What is the number of ICT systems (such as for example operating systems, databases systems, network systems, underlying software, excluding hardware, ATMs, mobile devices, etc.) for the entity/ies in scope (as of 31.12 of reference year)?	< # 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. >	No	
22a	Of which number of critical ICT systems (see glossary) for the entity/ies in scope? (as of 31.12 of reference year).	< # of critical ICT systems e.g. 500 >	< Please mention the 5 most critical systems of the entity/ies in scope. >	No	
23	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 reference year?	< # 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". >	No	< Select Overall Risk Level >
23a	Of which, number of changes 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'. >	No	
23b	Of which, number of changes that caused issues.	< # 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 >	No	
23c	What were the three main root causes of failure for changes that encountered issues, of which is reason number 1?	< 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. >	No	
23d	What were the three main root causes of failure for changes that encountered issues, of which is reason number 2?	< 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. >	No	
23e	What were the three main root causes of failure for changes that encountered issues, of which is reason number 3?	< 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. >	No	
24	How many critical audit, on-site inspection and internal model investigation findings related to ICT change risk have not been remediated for longer than 1 year (as of 31.12 of reference 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". >	No	
	ICT data integrity risk				
25	How many end user-developed applications (EUDA also known as EUC - End-User-Computing) support activities in total, including Microsoft Excel spreadsheets, Microsoft Access databases and other end user-developed tools (as of 31.12 of reference year)?	< # of end-user applications e.g. 215 >	< Please name business units with the highest number of end-user developed application supporting activities (e.g. ICT - 55; Risk Management 45; Credit Europe - 25). >	No	
25a	Of which, how many EUDAs support critical activities (e.g. regulatory reports such as FINREP/COREP, etc.)?	< # of end-user applications supporting critical activities e.g. 115 >	< Please name business units with the highest number of end-user developed application supporting critical activities (e.g. ICT - 55; Risk Management 45; Credit Europe - 25). Please clarify your definition of "critical". >	No	
26	How many incidents leading to significant invalid data modifications occurred in the reference year? Please note that this question refers to the number of ICT incidents related to data integrity?	< # of data integrity incidents e.g. 21 >	< Please briefly elaborate on the most significant invalid data modification incidents; please clarify your definition of "significant". >	No	
27	How many cases of incorrect data submission in the supervisory reporting occurred in the reference year? ~~Please note that this should at least include the number of resubmissions of ITS data in the Management Report on Data Governance and Data Quality.~~	< # of incorrect data submission cases >	< Please refer to the data collections listed in the simplifed SEP shared annually for supervisory reporting to be considered in this question; please briefly elaborate on the cases of incorrect data submission and the respective root causes. >	No	< Select Overall Risk Level >
27a	Of which, number of cases were due to ICT issues. ~~Please note that this number must be consistent with the qualitative answer given to question #4 in the annual Management Report on Data Governance and Data Quality.~~	< # of incorrect data submission cases due to ICT issues >	< Please briefly elaborate on the cases of incorrect data submission due to ICT issues and the respective root causes. >	No	
28	How many critical audit, on-site inspection and internal model investigation findings related to ICT data integrity risk have not been remediated for longer than 1 year (as of 31.12 of reference 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". >	No	
29	What was the total amount of losses due to data-related ICT-caused incidents (e.g. data breaches, data integrity, data quality, timeliness of reporting) (in €)?	< Overall amount of losses in € >	< Please mention the major loss drivers and root causes. >	No	

	Questions to the ICT Risk Level Unless specified otherwise, the question shall be answered in relation to the reference year	Answers	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	Has there been a material change of the definition of this item in comparison to last year's reporting?	Overall ICT Risk Level Self-Assessment
30	How many of the data quality issues reported internally have as cause ICT issues?	< # data quality issues e.g. 5 >	< Please explain the main ICT issues relevant here. >	No	
31	What is the percentage of critical or important functions among all for which golden sources of data are defined?	< Percentage of critical or important functions e.g. 60% >	< Please explain how the figure was derived. >	No	

	Questions to the ICT Risk Control Framework	Maturity levels	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	
	ICT Governance and ICT Risk Management		**Strengths**	**Weaknesses**
	ICT and digital operational resilience strategy			
1	1.1) A forward-looking, balanced ICT strategy is defined, documented, periodically updated, approved by the management body and aligned with the business and risk strategies (e.g. risk tolerance).	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	1.2) Senior management of the business line(s) is adequately involved in the definition of the supervised entity's strategic ICT priorities and aware of the development, design and initiation of major business strategies and initiatives.	< Maturity Level >		
	1.3) The ICT strategy provides a holistic view of the current ICT environment, the future direction, and the initiatives required to migrate to the desired future environment (incl. third party dependencies).	< Maturity Level >		
	1.4) The ICT strategy has an acceptable level of detail and contains measurable goals for the most important ICT areas.	< Maturity Level >		
	1.5) The ICT strategy is supported by concrete implementation plans (e.g. deliverables, important milestones and resource planning, dedicated budgets). The implementation plans are realistic and communicated to all relevant staff (including contractors and third party providers where applicable and relevant).	< Maturity Level >		
	1.6) Portfolios of ICT-enabled investment programs and projects required to achieve specific strategic business objectives are actively monitored by relevant stakeholders.	< Maturity Level >		
	1.7) The supervised entity analyses existing and emerging technologies.	< Maturity Level >		
	1.8) The ICT risk management framework includes a digital operational resilience strategy setting out how the framework shall be implemented. To that end, the digital operational resilience strategy includes methods to address ICT risk and attain specific ICT objectives, by: (a) explaining how the ICT risk management framework supports the financial entity's business strategy and objectives; (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; (c) setting out clear information security objectives, including key performance indicators and key risk metrics; (d) explaining the ICT reference architecture and any changes needed to reach specific business objectives; (e) outlining the different mechanisms put in place to detect ICT-related incidents, prevent their impact and provide protection from it; (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; (g) implementing digital operational resilience testing, in accordance with Chapter IV of Regulation (EU) 2022/2554; (h) outlining a communication strategy in the event of ICT-related incidents the disclosure of which is required in accordance with Article 14 of Regulation (EU) 2022/2554. The supervised entity 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 organization			
	2.1) The supervised entity has in place an internal governance and control framework that ensures an effective and prudent management of ICT risk, in accordance with Article 6(4) of Regulation (EU) 2022/2554, in order to achieve a high level of digital operational resilience.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "ICT group strategy 2015-2017"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "ICT group strategy 2015-2017"). >
	2.2) In accordance with Article 5(2) of Regulation (EU) 2022/2554, the management body of the supervised entity defines, approves, oversees and is responsible for the implementation of all arrangements related to the ICT risk management framework referred to in Article 6(1) of Regulation (EU) 2022/2554. In particular, the management body: (a) bears the ultimate responsibility for managing the financial entity's ICT risk; (b) puts in place policies that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality, of data; (c) sets 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; (d) bears the overall responsibility for setting and approving the digital operational resilience strategy as referred to in Article 6(8) of Regulation (EU) 2022/2554, including the determination of the appropriate risk tolerance level of ICT risk of the financial entity, as referred to in Article 6(8)(b) of Regulation (EU) 2022/2554; (e) approves, oversees and periodically reviews 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) of Regulation (EU) 2022/2554, 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; (f) approves and periodically reviews the financial entity's ICT internal audit plans, ICT audits and material modifications to them; (g) allocates and periodically reviews 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) of Regulation (EU) 2022/2554, and ICT skills for all staff; (h) approves and periodically reviews the financial entity's policy on arrangements regarding the use of ICT services provided by ICT third-party service providers; (i) puts in place, at corporate level, reporting channels enabling ICT to be duly informed of the following: (i) arrangements concluded with ICT third-party service providers on the use of ICT services, (ii) any relevant planned material changes regarding the ICT third-party service providers, (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.	< Maturity Level >		

	Questions to the ICT Risk Control Framework	Maturity levels	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	
2	2.3) Members of the management body of the supervised entity 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.	< Maturity Level >		
	2.4) The supervised entity includes in its human resource policy or other relevant policies all of the following ICT security related elements: (a) the identification and assignment of any specific ICT security responsibilities; (b) requirements for staff of the financial entity and of the ICT third-party service providers using or accessing ICT assets of the financial entity to: (i) be informed about, and adhere to, the financial entity's ICT security policies, procedures, and protocols; (ii) be aware of the reporting channels put in place by the financial entity for the detection of anomalous behaviour, including, where applicable, the reporting channels established in line with Directive (EU) 2019/1937 of the European Parliament and of the Council; (iii) for the staff, to return to the financial entity, upon termination of employment, all ICT assets and tangible information assets in their possession that belong to the financial entity.	< Maturity Level >		
	2.5) As part of the ICT risk management framework referred to in Article 6(1) of Regulation (EU) 2022/2554, the supervised entity has identified, classified and adequately documented 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. The supervised entity reviews as needed, and at least yearly, the adequacy of this classification and of any relevant documentation.	< Maturity Level >		
	2.6) The supervised entity maintains an inventory of 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. This inventory is updated periodically and every time any major change in the network and information system infrastructure, in the processes or procedures affecting its ICT supported business functions, information assets or ICT assets occurs.	< Maturity Level >		
	2.7) The supervised entity has identified all information assets and ICT assets, including those on remote sites, network resources and hardware equipment, and maps those considered critical. The supervised entity has mapped the configuration of the information assets and ICT assets and the links and interdependencies between the different information assets and ICT assets.	< Maturity Level >		
	2.8) The supervised entity maintains an inventory of all information assets and ICT assets, including those on remote sites, network resources and hardware equipment. This inventory is updated periodically and every time any major change in the network and information system infrastructure, in the processes or procedures affecting its ICT supported business functions, information assets or ICT assets occurs.	< Maturity Level >		
	2.9) The supervised entity maintains an inventory of all processes that are dependent on ICT third-party service providers, and identified interconnections with ICT third-party service providers that provide services that support critical or important functions. This inventory is updated periodically and every time any major change in the network and information system infrastructure, in the processes or procedures affecting its ICT supported business functions, information assets or ICT assets occurs.	< Maturity Level >		
	2.10) The supervised entity conducts on a regular basis, and at least yearly, a specific ICT risk assessment on all legacy ICT systems and, in any case before and after connecting technologies, applications or systems.	< Maturity Level >		
	ICT risk management framework			
	3.1) The supervised entity has in place a sound, comprehensive and well-documented ICT risk management framework as part of its overall risk management system, which enables it to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	3.2) The ICT risk management framework includes 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.	< Maturity Level >		
	3.3) The supervised entity performs a risk assessment upon each major change in the network and information system infrastructure, in the processes or procedures affecting its ICT supported business functions, information assets or ICT assets.	< Maturity Level >		
	3.4) The supervised entity has, in the context of the digital operational resilience strategy referred to in Article 6(8) of Regulation (EU) 2022/2554, defined 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.	< Maturity Level >		
	3.5) The supervised entity assigns the responsibility for managing and overseeing ICT risk to a control function and ensures an appropriate level of independence of such control function in order to avoid conflicts of interest. The supervised entity ensures 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.	< Maturity Level >		
	3.6) The supervised entity performs post incident review after major ICT-related incidents (in accordance with the requirements of Article 13(2) of Regulation (EU) 2022/2554.	< Maturity Level >		
	3.7) Senior ICT staff reports at least annually to the management body on important findings and lessons (incl. remediation recommendations). These findings and lessons are derived from, among other sources: post incident reviews, digital operational resilience testing, along with challenges faced upon the activation of ICT business continuity plans and ICT response and recovery plans.	< Maturity Level >		
	3.8) The supervised entity's ICT risk management policies and procedures contain an indication of the approval of the risk tolerance level for ICT risk established in accordance with Article 6(8)(b), of Regulation (EU) 2022/2554.	< Maturity Level >		

	Questions to the ICT Risk Control Framework	Maturity levels	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	
3	3.9) The supervised entity's ICT risk management policies and procedures contain a procedure and a methodology to conduct the ICT risk assessment, identifying: (i) vulnerabilities and threats that affect or may affect the supported business functions, the ICT systems and ICT assets supporting those functions; (ii) the quantitative or qualitative indicators to measure the impact and likelihood of the vulnerabilities and threats referred to in point (i).	< Maturity Level >		
	3.10) The supervised entity's ICT risk management policies and procedures contain the procedure to identify, implement, and document ICT risk treatment measures for the ICT risks identified and assessed, including the determination of ICT risk treatment measures necessary to bring ICT risk within the risk tolerance level. The procedure ensures (a) the monitoring of the effectiveness of the ICT risk treatment measures implemented; (b) the assessment of whether the established risk tolerance levels of the financial entity have been attained; (c) the assessment of whether the financial entity has taken actions to correct or improve those measures where necessary.	< Maturity Level >		
	3.11) The supervised entity's ICT risk management policies and procedures contain for the residual ICT risks that are still present following the implementation of the ICT risk treatment measures: (i) provisions on the identification of those residual ICT risks; (ii) the assignment of roles and responsibilities regarding: (1) the acceptance of the residual ICT risks that exceed the financial entity's risk tolerance level; (2) for the review process referred to in point (iv) below; (iii) the development of an inventory of the accepted residual ICT risks, including a justification for their acceptance; (iv) provisions on the review of the accepted residual ICT risks at least once a year, including: (1) the identification of any changes to the residual ICT risks; (2) the assessment of available mitigation measures; (3) the assessment of whether the reasons justifying the acceptance of residual ICT risks are still valid and applicable at the date of the review.	< Maturity Level >		
	3.12) The supervised entity's ICT risk management policies and procedures contain provisions on the monitoring of: (i) any changes to the ICT risk and cyber threat landscape; (ii) internal and external vulnerabilities and threats; (iii) new technological developments, with a view to understanding their potential impact on ICT risk, digital operational resilience and security requirements; (iv) ICT risk of the financial entity that enables prompt detection of changes that could affect its ICT risk profile.	< Maturity Level >		
	3.13) The supervised entity's ICT risk management policies and procedures contain provisions on a process to ensure that any changes to the business strategy and the digital operational resilience strategy of the financial entity are taken into account.	< Maturity Level >		
	3.14) The supervised entity, 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 supervised entity reviews on a regular basis, and at least yearly, the risk scenarios impacting it.	< Maturity Level >		
	ICT Internal audit (3LoD)			
4	4.1) The ICT risk management framework is documented and reviewed at least once a year, 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. ICT is continuously improved on the basis of lessons derived from implementation and monitoring. A comprehensive and detailed ICT audit universe is established.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	4.2) The ICT risk management framework is subject to internal audit by auditors on a regular basis in line with the supervised entity's audit plan. The auditors possess sufficient knowledge, skills and expertise in ICT risk, as well as appropriate independence.	< Maturity Level >		
	4.3) The audit plan includes critical ICT risks identified by the supervised entity (including those of outsourced activities) and takes into consideration the results of previous audits. The frequency and focus of ICT audits is commensurate to the ICT risk of the financial entity.	< Maturity Level >		
	4.4) Based on the conclusions from the internal audit review, the supervised entity has established a formal follow-up process, including rules for the timely verification and remediation of critical ICT audit findings and progress reports being periodically reviewed by the senior management and/or the audit committee.	< Maturity Level >		
	4.5) There is procedure for ad hoc reporting to the management body based on the criticality of the findings reported by ICT audits.	< Maturity Level >		
	ICT reporting			
5	5.1) An ICT reporting process is designed with clear structural and operational rules, defining responsibilities, subjects of reports, deadlines, communication channels, etc. and ensuring that the ICT reporting is performed with the appropriate level of accuracy, integrity, completeness, comprehensiveness, clarity, usefulness and timeliness.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope.	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope.
	5.2) Secured channels are used for the distribution of ICT reports.	< Maturity Level >		

	Questions to the ICT Risk Control Framework	Maturity levels	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	
	5.3) The ICT reporting system includes the reporting of the ICT service provider (e.g. cloud service provider), in case of an outsourced activity.	< Maturity Level >	In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	5.4) ICT reporting is performed on a regular basis, providing information to relevant recipients (e.g. senior management) to identify, assess, monitor and manage the supervised entity's ICT risk considering the approved risk appetite.	< Maturity Level >		
	ICT third party management		**Strengths**	**Weaknesses**
	Overall risk profile and complexity			
6	6.1) As part of its ICT risk management framework, the supervised entity adopts, and regularly reviews a strategy on ICT third-party risk, taking into account the multi-vendor strategy referred to in Article 6(9) of Regulation (EU) 2022/2554, where applicable. The strategy on ICT third-party risk includes a policy on the use of ICT services supporting critical or important functions provided by ICT third-party service providers (the ICT TP usage policy) and applies on an individual basis and, where relevant, on a sub-consolidated and consolidated basis. The management body, on the basis of an assessment of the overall risk profile of the supervised entity and the scale and complexity of the business services, regularly reviews the risks identified in respect to contractual arrangements on the use of ICT services supporting critical or important functions.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	6.2) As part of its ICT risk management framework, the supervised entity maintains and updates 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 are appropriately documented, distinguishing between those that cover ICT services supporting critical or important functions and those that do not.	< Maturity Level >		
	6.3) The ICT TP usage policy takes into account the size and the overall risk profile of the supervised entity, and the nature, scale and elements of increased or reduced complexity of its services, activities and operations, including elements relating to: (a) the type of ICT services included in the contractual arrangement on the use of ICT services supporting critical or important functions provided by ICT third-party service providers (the 'contractual arrangement') between the supervised entity and the ICT third-party service provider; (b) the location of the ICT third-party service provider or the location of its parent company; (c) whether the ICT services supporting critical or important functions are provided by an ICT third-party service provider located within a Member State or in a third country, also considering the location from where the ICT services are provided and the location where the data is processed and stored.	< Maturity Level >		
	6.4) The policy takes into account the size and the overall risk profile of the supervised entity, and the nature, scale and elements of increased or reduced complexity of its services, activities and operations, including elements relating to: (a) the nature of the data shared with the ICT third-party service provider; (b) whether the ICT third-party service provider is part of the same group as the supervised entity to which the services are provided; (c) the use of ICT third-party service providers that are authorised, registered or subject to supervision or oversight by a competent authority in a Member State or subject to the oversight framework under Chapter V, Section II, of Regulation (EU) 2022/2554, and the use of ICT third-party service providers that are not.	< Maturity Level >		
	6.5) The ICT TP usage policy takes into account the size and the overall risk profile of the supervised entity, and the nature, scale and elements of increased or reduced complexity of its services, activities and operations, including elements relating to: (a) the use of ICT third-party service providers that are authorised, registered or subject to supervision or oversight by a supervisory authority in a third country, and the use of ICT third-party service providers that are not; (b) whether the provision of ICT services supporting critical or important functions are concentrated to a single ICT third-party service provider or a small number of such service providers; (c) the transferability of the ICT services supporting critical or important functions to another ICT third-party service provider, including as a result of technology specificities; (d) the potential impact of disruptions in the provision of the ICT services supporting critical or important functions on the continuity of the supervised entity's activities and on the availability of its services.	< Maturity Level >		
	Governance of ICT Third Party arrangements			
	7.1) The management body reviews the ICT TP usage policy at least once a year and update it where necessary. Changes made to the policy are implemented in a timely manner and as soon as it is possible within the relevant contractual arrangements. The supervised entity documents the planned timeline for the implementation.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	7.2) The ICT TP usage policy establishes or refers to a methodology for determining which ICT services support critical or important functions. The policy also specifies when this assessment is to be conducted and reviewed.	< Maturity Level >		
	7.3) The ICT TP usage policy clearly assigns the internal responsibilities for the approval, management, control, and documentation of relevant contractual arrangements and ensures that appropriate skills, experience and knowledge are maintained within the supervised entity to effectively oversee the relevant contractual arrangements, including the ICT services provided under those arrangements.	< Maturity Level >		
	7.4) The ICT TP usage policy clearly identifies the role or member of senior management responsible for monitoring the relevant contractual arrangements. The policy specifies how that role or member of senior management cooperates with the control functions, unless ICT is part of it, and sets out the reporting lines to the management body, including the nature of the information to report and the documents to provide. ICT also sets out the frequency of such reporting.	< Maturity Level >		

	Questions to the ICT Risk Control Framework	Maturity levels	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	
7	7.5) The ICT TP usage policy ensures that the contractual arrangements are consistent with the following: (a) the ICT risk management framework referred to in Article 6 of Regulation (EU) 2022/2554; (b) the information security policy referred to in Article 9(4) of Regulation (EU) 2022/2554; (c) the ICT business continuity policy referred to in Article 11 of Regulation (EU) 2022/2554; (d) the requirements on incident reporting set out in Article 19 of Regulation (EU) 2022/2554.	< Maturity Level >		
	7.6) The ICT TP usage policy requires that ICT services supporting critical or important functions provided by ICT third party service providers are subject to independent review and are included in the audit plan.	< Maturity Level >		
	7.7) The ICT TP usage policy explicitly specifies that the contractual arrangements: (a) do not relieve the supervised entity and its management body of its regulatory obligations and its responsibilities to its clients; (b) are not to prevent effective supervision of a supervised entity 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 supervised entity, 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 >		
	7.8) For ICT assets or services operated by an ICT third-party service provider, the supervised entity 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) of the RTS on ICT risk management framework.	< Maturity Level >		
	Main phases of the life cycle for the adoption and use of contractual arrangements			
8	8.1) The ICT TP usage 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 to specify the policy on ICT services and the approval process regarding new or material changes to contractual arrangements as set out in Article 8(4) of the RTS to specify the policy on ICT services. The risk assessment is done at financial entity level and, where applicable, at consolidated and sub-consolidated level before a contractual arrangement is concluded. The risk assessment takes into account all the relevant requirements laid down in Regulation (EU) 2022/2554, and all the risk posed by the provision of ICT services as detailed in article 5 para. 2 of the RTS to specify the policy on ICT services. 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 >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	8.2) The ICT TP usage 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 arrangements; (b) the implementation, monitoring and management of contractual arrangements as referred to in Articles 7, 8 and 9 of the RTS to specify the policy on ICT services, including at consolidated and sub-consolidated level, where applicable.	< Maturity Level >		
	8.3) The ICT TP usage 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 documentation and record-keeping, taking into account the requirements with regard to the register of information laid down in Article 28(3) of Regulation (EU) 2022/2554; (b) the exit strategies and termination processes as set out in Article 10 of the RTS to specify the policy on ICT services.	< Maturity Level >		
	8.4) The ICT TP usage 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 financial entity 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 financial entity or other information provided by the ICT third-party service provider.	< Maturity Level >		
	Conflict of Interests			
9	9.1) The ICT TP usage policy specifies the appropriate measures to identify, prevent and manage actual or potential conflicts of interests arising from the use of ICT third-party service providers before entering relevant contractual arrangements and provide for an ongoing monitoring of conflicts of interests.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment
	9.2) Where ICT services are provided by ICT intra-group service providers, the ICT TP usage policy specifies that decisions on conditions, including the financial conditions, for the ICT services supporting critical or important functions are taken objectively.	< Maturity Level >		
	Contractual clauses for the use of ICT services supporting critical or important functions			
	10.1) The ICT TP 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 >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and

	Questions to the ICT Risk Control Framework	Maturity levels	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	
10	10.2) The ICT TP usage policy specifies that the relevant contractual arrangements shall include information access, inspection, audit, and ICT testing rights. The policy foresees that without prejudice to the final responsibility of the supervised entity, the supervised entity shall use for this purpose: (a) its own internal audit or an appointed third party; (b) where appropriate, pooled audits and pooled ICT testing, including threat-led penetration testing, organised jointly with other contracting financial entities or firms that use ICT services of the same ICT third-party service provider, that are performed by them and these contracting financial entities or firms or by a third party appointed by them; (c) where appropriate, third-party certifications (d) where appropriate third-party or internal audit reports made available by the ICT third-party service provider.	< Maturity Level >	explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	10.3) The supervised entity does not rely solely on certifications as in 10.2 (c) or reports as in 10.2 (d) over time unless: (a) is satisfied with the audit plan of the ICT service third-party provider for the relevant contractual arrangements; (b) ensures that the scope of the certifications or audit reports cover the systems and key controls identified by the financial entity and the compliance with relevant regulatory requirements; (c) thoroughly assesses the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are not obsolete; (d) ensures that key systems and controls are covered in future versions of the certification or audit report; (e) is satisfied with the aptitude of the certifying or auditing party; (f) is satisfied that the certifications are issued, and the audits are performed against widely recognised relevant professional standards and include a test of the operational effectiveness of the key controls in place; (g) has the contractual right to request the expansion of the scope of the certifications or audit reports to other relevant systems and controls; whereby the number and frequency of such requests for scope modification shall be reasonable and legitimate from a risk management perspective; and (h) retains the contractual right to perform individual and pooled audits at its discretion with regard to the relevant contractual arrangements and execute them in line with the contracted frequency.	< Maturity Level >		
	10.4) The ICT TP usage 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.	< Maturity Level >		
	Monitoring of the contractual arrangements for the use of ICT services supporting critical or important functions and exit/termination			
11	11.1) The ICT TP usage policy ensures that the relevant contractual arrangements specify the measures and key indicators to monitor, on an ongoing basis, to assess the performance of ICT third party service providers, including measures to monitor compliance with requirements regarding the confidentiality, availability, integrity and authenticity of data and information, and the compliance of the ICT third-party service providers with the financial entity's relevant policies and procedures. The policy also specifies measures that apply when service level agreements are not met including, where appropriate contractual penalties.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	11.2) The ICT TP usage policy prescribes how the supervised entity shall assess that the ICT third party service providers used for the ICT services supporting critical or important functions meets appropriate performance and quality standards in line with the contractual arrangement and the supervised entity's own policies by ensuring that: (a) the ICT third-party service providers address appropriate reports on their activities and services provided to the supervised entity, including periodic reports, incidents reports, service delivery reports, reports on ICT security and on business continuity measures and testing; (b) the performance of ICT third-party service providers is assessed with key performance indicators, key control indicators, audits, self-certifications and independent reviews in line with the financial entity's ICT risk management framework; (c) other relevant information is received from the ICT third-party service provider; (d) the supervised entity is notified, where appropriate, of ICT- related incidents and operational or security payment related incidents; (e) an independent review and compliance audits with legal and regulatory requirements and policies are performed.	< Maturity Level >		
	11.3) The ICT TP usage policy prescribes that the assessment referred to in 11.2 should be documented and its results should be used to update the supervised entity's risk assessment.	< Maturity Level >		
	11.4) The ICT TP usage policy defines the appropriate measures that the supervised entity shall adopt if ICT identifies shortcomings of the ICT third-party service provider, including ICT-related incidents and operational or security payment related incidents, in the provision of the ICT services supporting critical or important functions or the compliance with contractual arrangements or legal requirements and how the implementation of such measures shall be monitored to ensure that they are effectively complied within a defined timeframe, taking into account the materiality of the shortcomings.	< Maturity Level >		
	11.5) Without prejudice to Article 28 (7) and (8) of Regulation (EU) 2022/2554, the policy includes requirements for a documented exit plan for each ICT contractual arrangement on ICT services supporting critical or important functions provided by an ICT third-party service provider and its periodic review and testing, taking into account unforeseen and persistent service interruptions, inappropriate or failed service delivery or the unexpected termination of a relevant contractual arrangement. The supervised entity has ensured that the exit plan is realistic, feasible, based on plausible scenarios and reasonable assumptions and shall have a planned implementation schedule compatible with the exit and termination terms established in the relevant contractual arrangements.	< Maturity Level >		
	Information Security Management		**Strengths**	**Weaknesses**
	Information security policies, standards, guidelines and awareness			
	12.1) The supervised entity has established an information security policy approved by the management body and aligned to the information security objectives included in the digital operational resilience strategy.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the	< Please explain why you chose the respective overall maturity level. If there are important variations within the

	Questions to the ICT Risk Control Framework	Maturity levels	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	
12	12.2) The information security policy sets the rules to protect the supervised entity's information assets, in line with its strategy and risk appetite and is applicable to all employees and third parties accessing information.	< Maturity Level >	entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	12.3) The information security policy 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, including via the use of cryptographic techniques; iv) guarantying an accurate and prompt data transmission without major disruptions and undue delays.	< Maturity Level >		
	12.4) The information security policy is communicated to all staff at all levels and contractors and its implementation is supported by appropriate investments in human and technical resources.	< Maturity Level >		
	12.5) The information security policy specifies the consequences of non-compliance by staff of the financial entity, lists the documentation to be maintained and specifies the segregation of duties arrangements with respect to information security controls.	< Maturity Level >		
	12.6) The supervised entity has put in place indicators to monitor the implementation of the ICT security policy and exceptions from it.	< Maturity Level >		
	12.7) The supervised entity 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 institution'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 >		
	12.8) There are regular (at least annually) information security awareness and information campaigns in place to inform all employees and contractors of the supervised entity. Explaining the safe use and protection of the supervised entity's ICT systems and the main ICT security (and other) risks they should be aware of, including in particular cyber threats (e. g. computer viruses, possible internal or external abuses or attacks, cyber-attacks) and their role in mitigating security breaches. Levels of understanding are measured and gaps in knowledge are identified and used to adapt or prompt additional training.	< Maturity Level >		
	12.9) Newcomers receive mandatory training on ICT security.	< Maturity Level >		
	12.10) ICT staff receives specific trainings on ICT security.	< Maturity Level >		
	12.11) All employees (including senior management staff) receives compulsory digital operational resilience training, with complexity commensurate to the individual's role/function. This may also extent to ICT third- party providers, as per Article 13(6) of Regulation (EU) 2022/2554.	< Maturity Level >		
	12.12) The Intranet site has a dedicated section on ICT security topics, guidelines and best practices.	< Maturity Level >		
	12.13) Requirements on confidentiality or non-disclosure arrangements reflecting the financial entity's needs for the protection of information for both the staff of the financial entity and of third parties are implemented, documented, and regularly reviewed.	< Maturity Level >		
	Identity and access management (IAM)			
	13.1) As part of their control of access management rights, financial entity develops, documents, and implements identity and access management policies and procedures. Identity management ensures unique identification and authentication of natural persons and systems accessing the financial entities' information to enable assignment of user access rights .	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have

	Questions to the ICT Risk Control Framework	Maturity levels	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	
13	13.2) The identity and access management policies and procedures cover all of the following: * unique identity corresponding to a unique user account is assigned to each staff member of the financial entity or staff of the ICT third-party service providers accessing the information assets and ICT assets of the financial entity. 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; * records of all identity assignments are maintained, in compliance with the applicable retention requirements. Those records shall be kept following a reorganisation of the financial entity or after the end of the contractual relationship. * 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 >	been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	13.3) The identity and access management policies and procedures cover all of the following: * 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. * The segregation of duties designed to prevent unjustified access to critical data or to prevent the allocation of combinations of access rights that may be used to circumvent controls. * A provision on restrictions of access to ICT assets, setting out controls and tools to prevent unauthorised access. * Account management procedures to grant, change or revoke access rights for user and generic accounts, including generic administrator accounts, including provision on all of the following: (i) Assignment of roles and responsibilities for granting, reviewing, and revoking access rights. Retention period is established, taking into account the business and information security objectives, the reasons for recording the event in the logs, and the results of the ICT risk assessment. (ii) Assignment of privileged, emergency, and administrator access on a need-to-use or an ad-hoc basis for all ICT systems. Where possible, dedicated accounts are used for the performance of administrative tasks on ICT systems. Where feasible and appropriate, automated solutions are deployed for the privilege access management. (iii) Withdrawal of access rights without undue delay upon termination of the employment or when the access is no longer necessary. (iv) Update of access rights where changes are necessary and at least once a year for all ICT systems, other than ICT systems supporting critical or important functions and at least every 6 months for ICT systems supporting critical or important functions.	< Maturity Level >		
	13.4) The identity and access management policies and procedures cover all of the following: * Authentication methods, including: (i) the use of authentication methods commensurate to the classification established in accordance with Article 8(1) of Regulation (EU) 2022/2554 and to the overall risk profile of ICT assets and considering leading practices; (ii) the use of strong authentication methods in accordance with leading practices and techniques for remote access to the financial entity's network, for privileged access, for access to ICT assets supporting critical or important functions or ICT assets that are publicly accessible; * Physical access controls measures including: (i) The identification and logging of natural persons that are authorised to access premises, data centres, and sensitive designated areas identified by the financial entity where ICT and information assets reside. The identification and logging is commensurate with the importance of the premises, data centres, sensitive designated areas, and the criticality of the operations or ICT systems located therein. (ii) The granting of physical access rights to critical ICT assets to authorised persons only, in accordance with the need-to-know and least privilege principles, and on an ad-hoc basis. (iii) The monitoring of physical access to premises, data centres, and sensitive designated areas identified by the financial entity where ICT and information assets or both reside. The monitoring shall be commensurate to the classification established in accordance with Article 8(1) of Regulation (EU) 2022/2554 and the criticality of the area accessed. (iv) The review of physical access rights to ensure that unnecessary access rights are promptly revoked.	< Maturity Level >		
	13.5) ICT and security related requirements of the EBA/GL/2022/15 on Remote Customer Onboarding Solutions are implemented (in particular, para. 51-53).	< Maturity Level >		
	Patch and vulnerability management, security reviews			
	14.1) Patch and vulnerability management is developed and implemented.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	14.2) All patching processes are triggered and performed in timely manner.	< Maturity Level >		
	14.3) Vulnerabilities are identified (incl. through vulnerability scanning), centrally documented, analysed, classified and patched accordingly within an acceptable timeframe, coherent with the ICT systems' criticality.	< Maturity Level >		

	Questions to the ICT Risk Control Framework	Maturity levels	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	
14	14.4) Security reviews on the general information security controls, processes and procedures are carried out regularly (at least annually for critical systems and every 3 years for non-critical systems).	< Maturity Level >		
	14.5) Security reviews cover the logical security (e.g. application and operating system level) including penetration testing of the interfaces or applications treating sensitive information or having a large impact in case of compromise.	< Maturity Level >		
	14.6) Similarly, physical security (incl. appropriate redundancy levels) is regularly reviewed against best practices.	< Maturity Level >		
	14.7) In order to provide objective and reliable results, security reviews are carried out by independent parties to maintain segregation of duties.	< Maturity Level >		
	Network and end-point security (incl. remote access)			
15	15.1) The supervised entity has, as part of the safeguards ensuring the security of networks against intrusions and data misuse, developed, documented, and implemented policies, procedures, protocols, and tools on network security management.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	15.2) The policies, procedures, protocols, and tools on network security management cover: * the segregation and segmentation of ICT systems and networks * the use of a separate and dedicated network for the administration of ICT assets; * the identification and implementation of network access controls to prevent and detect connections to the financial entity's network by any unauthorised device or system, or any endpoint not meeting the financial entity's security requirements; * the measures to temporarily isolate, where necessary, subnetworks, and network components and devices.	< Maturity Level >		
	15.3 The policies, procedures, protocols, and tools on network security management cover: * the encryption of network connections (internal and external); * the management and review of firewall rules and connections filters; * the securing of network traffic between the internal networks and the internet and other external connections; * the procedures to limit, lock, and terminate system and remote sessions after a specified period of inactivity.	< Maturity Level >		
	15.4) The policies, procedures, protocols, and tools on network security management cover: * the documentation of all of the financial entity's network connections and data flows; * the design of networks in line with the established ICT security requirements; * the performance of reviews of the network architecture and of the network security design to identify potential vulnerabilities; * the implementation of a secure configuration baseline of all network components, and the hardening of the network and of network devices.	< Maturity Level >		
	15.5) The policies, procedures, protocols, and tools on network security management cover: * the identification and specification of ICT and information security measures, service levels, and management requirements of all network services (whether intra-group or external).	< Maturity Level >		
	15.6) The supervised entity implemented appropriate policies, procedures, protocols and tools to protect data during network transmission and to assess compliance with the respective requirements.	< Maturity Level >		
	15.7) Any maintenance is properly logged, including remote maintenance.	< Maturity Level >		
	15.8) The supervised entity has implemented adequate protection against malware (e.g. antivirus, advanced malware prevention solutions, sandboxes).	< Maturity Level >		
	15.9) The malware prevention technologies 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). For example, malware prevention on mobile devices can be achieved by equivalent lockdown and monitoring measures in accordance with the current industry best practice.	< Maturity Level >		
	15.10) The malware prevention software is updated regularly and technical measures prevent end users from deactivating this.	< Maturity Level >		
	15.11) The supervised entity has implemented appropriate procedures and security controls to secure the use of portable endpoint devices and private non-portable endpoint devices (in accordance with the requirements of the Article 11(2)(f) and (j) of the RTS on ICT risk management.	< Maturity Level >		
	15.12) The supervised entity has implemented data protection procedures, protocols and tools (in accordance with the requirements of the Article 11(2)(e), (g) and (h) of RTS on ICT risk management.	< Maturity Level >		

	Questions to the ICT Risk Control Framework	Maturity levels	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	
	Security event logging and monitoring			
16	16.1) As part of the safeguards against intrusions and data misuse, logging procedures, protocols and tools have been developed, documented, and implemented. The logging procedures, protocols, and tools contains all of the requirements in article 12(2) of the RTS on ICT risk management framework.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	16.2) Efficiency of Security event logging and monitoring (SIEM) process is increased by the use of supporting technologies to correlate security events (e.g. Security Incident Event Management) and/or the use of dedicated teams (e.g. SOC - Security Operating Centre, CERT - Computer Emergency Response Team).	< Maturity Level >		
	16.3) Security events generating an alert are promptly managed/treated via a coordinated security incident management process.	< Maturity Level >		
	16.4) A cybersecurity incident response plan, which describes how to react in case of a cybersecurity incident, incorporating lessons learned, is in place and regularly updated.	< Maturity Level >		
	16.5) The supervised entity collaborates 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 >		
	16.6) The Senior Management is timely informed about the ICT security incidents detected in the organisation including their consequences, organisation reaction and additional controls implemented..	< Maturity Level >		
	Physical access and environmental controls			
17	17.1) As part of the safeguards to preserve the availability, authenticity, integrity, and confidentiality of data, a physical and environmental security policy is defined, documented, and implemented. This policy is designed taking into account the cyber threat landscape, in accordance with the classification established in accordance with Article 8(1) of Regulation (EU) 2022/2554, and in light of the overall risk profile of ICT assets and accessible information assets.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	17.2) The physical and environmental security policy contains measures to protect from attacks, accidents, and environmental threats and hazards, the premises, data centres of the financial entity, and sensitive designated areas identified by the financial entity, where ICT assets and information assets reside;	< Maturity Level >		
	17.3) The physical and environmental security policy covers the following: * measures to secure ICT assets, both within and outside the premises of the financial entity, taking into account the results of the ICT risk assessment related to the relevant ICT assets and commensurate with their importance; * measures to ensure the availability, authenticity, integrity, and confidentiality of ICT assets, information assets, and physical access control devices of the financial entity through the appropriate maintenance (including measures to protect unattended ICT assets).	< Maturity Level >		
	17.4) The physical and environmental security policy contains measures to preserve the availability, authenticity, integrity, and confidentiality of the data, including: * a clear desk policy for papers; * a clear screen policy for information processing facilities.	< Maturity Level >		
	Data classification			
18	18.1) The supervised entity maintains documented, approved and enforced data classification policies and procedures, describing how to classify information based on confidentiality, integrity, availability and legal/ regulatory requirements (e.g. data protection).	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	18.2) In order to properly conduct the data classification, clear owners of the information (categories) are determined.	< Maturity Level >		
	18.3) Data classification policies and procedures describe what measures are applied based on the classified criticality/sensitivity of the information and take into consideration the complete lifecycle of the ICT assets (e.g. measures applied when replacing, archiving, discarding or destroying ICT systems).	< Maturity Level >		
	18.4) 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.	< Maturity Level >		
	ICT Operations		**Strengths**	**Weaknesses**
	ICT asset inventory and configuration management			

	Questions to the ICT Risk Control Framework	Maturity levels	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	
19	19.1) The supervised entity maintains 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 >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	19.2) The inventory identifies the critical assets and the corresponding recovery requirements, and the interdependencies/ data flows between different assets.	< Maturity Level >		
	19.3) Secure configuration baselines for ICT assets that minimise exposure of those ICT assets to cyber threats are established by defining a set of standard configuration setups and hardening rules and also measures to verify regularly that those baselines are effectively deployed. The supervised entity should have implemented security measures to ensure that only authorised software is installed according to Article 11 of the RTS on ICT risk management framework.	< Maturity Level >		
	19.4) The supervised entity has implemented security measures to ensure that only authorised software is installed in accordance with Article 11(2)(c) of the RTS on ICT risk management..	< Maturity Level >		
	Availability and capacity management			
20	20.1) The supervised entity backs up its ICT systems in line with a predefined backup policy, taking into account the applicable regulatory requirements, business recovery requirements, and the criticality of the underlying systems.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	20.2) To ensure availability in case of disasters, backups are also stored at a different off-site location and sufficiently remote from the main one/primary hosting the ICT systems.	< Maturity Level >		
	20.3) The management of the offsite storage facility complies with the data classification policy and the supervised entity's media storage practices.	< Maturity Level >		
	20.4) Depending on the sensitivity of the information involved, backups are encrypted to protect the information in case of loss or voluntary/accidental alteration.	< Maturity Level >		
	20.5) Backups are regularly tested to ensure they are not corrupted.	< Maturity Level >		
	20.6) The supervised entity has documented and implemented procedures to ensure the standard operations of its ICT systems. Such procedures include (but not limited to): job scheduling processes; logging and monitoring of ICT systems (systems are monitored at all times and automatic alerts are sent to dedicated teams ensuring continuous operations) allowing the detection, analysis and correction of errors, etc.	< Maturity Level >		
	20.7) There exists capacity management monitoring processes to ensure system resources (e.g. CPU, RAM, Hard Disk space ...) are always in line with application(s) needs, they can cope with performance peaks and the supporting ICT assets are regularly reviewed, maintained and repaired as befitting their criticality.	< Maturity Level >		
	20.8) Where applicable, there are appropriate shift handover processes (formal handover of activity, status updates, operational problems, escalation procedures and reports on current responsibilities) in order to support agreed-upon service levels and ensure continuous operations.	< Maturity Level >		
	Incident and problem management			
21	21.1) A documented process providing guidance on incident management is in place, which includes definition of roles and responsibilities such as the members of the crisis committee(s), as well as escalation procedures (i.e. chain of command in case of emergency).	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	21.2) Incidents and service requests are identified, logged (by way of dedicated service desk tools), categorized and prioritised according to business criticality and service agreements.	< Maturity Level >		
	21.3) Notifications from detection systems are investigated in a timely manner and when required, response plans are swiftly executed and forensics are performed.	< Maturity Level >		
	21.4) Major incidents are escalated to timely convey information for risk management and decision-making processes and may result in the activation of a disaster recovery/ business continuity plan.	< Maturity Level >		
	21.5) If required, escalation might involve notification to relevant authorities.	< Maturity Level >		
	21.6) A documented problem management process is in place, in order to identify and solve the common root cause and prevent future incidents from occurring by for example the use of early warning indicators. There is guidance on problem management processes, including definition of roles and responsibilities in case of escalation and/or crises, when the members of the crisis committee(s) are known, and the chain of command is known in case of security emergencies.	< Maturity Level >		

	Questions to the ICT Risk Control Framework	Maturity levels	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	
	ICT change and release management			
22	22.1) A formal and documented process is in place for managing and controlling changes to ICT systems.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	22.2) Changes are defined, prioritised, formally approved, planned, tested and transitioned in a consistent and coordinated way.	< Maturity Level >		
	22.3) Significant changes are scheduled for implementation and approved by a dedicated management committee.	< Maturity Level >		
	22.4) Segregation of duties is applied throughout the different phases of the change process. In particular, development and testing are carried out on dedicated environments which are separated from the production environment.	< Maturity Level >		
	22.5) Development and test environments do not contain confidential production data and test environments adequately reflect the production environment.	< Maturity Level >		
	22.6) The deployment of changes into production environment is only conducted by authorised production teams after a formal change approval.	< Maturity Level >		
	22.7) Changes to ICT security controls (e.g. to firewall rules) are authorised by relevant Information/ICT security managers (e.g. CISO) after having analysed the ICT security impacts.	< Maturity Level >		
	22.8) A procedure is in place in order to manage emergency changes (changes requiring a quicker implementation due to critical/ blocking incidents) in a controlled environment and only upon formal documented approval.	< Maturity Level >		
	22.9) A release management team that directs the ICT departments' decisions about production setting, ensuring a holistic view of changes to ICT systems, is in place.	< Maturity Level >		

	Questions to the ICT Risk Control Framework	Maturity levels	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	
	Software Acquisition, Software Development and Project Management		**Strengths**	**Weaknesses**
	ICT project management framework (including governance)			
23	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 >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	23.2) Project governance and oversight processes are implemented to effectively support the management and monitoring of ICT projects (e.g. project management office, an ICT steering committee or equivalent) and include appropriate reporting of the establishment and progress of ICT projects and their associated risks to the management body at an adequate frequency.	< Maturity Level >		
	23.3) Project oversight for the development of any critical system is assigned to the ICT steering committee.	< Maturity Level >		
	23.4) The projects of the supervised entity are consistent with its strategy.	< Maturity Level >		
	23.5) The projects are initiated with an approved scope, benefits, objectives and identified key stakeholders.	< Maturity Level >		
	23.6) Dependencies between projects are identified, analysed, evaluated and managed by an overarching function.	< Maturity Level >		
	23.7) A project independent quality assurance is implemented.	< Maturity Level >		
	ICT projects			
24	24.1) ICT standards and methodologies are defined and implemented to effectively govern and document the process of developing (including agile development and DevOps approach), acquiring, implementing and maintaining information systems and related technology (including technology infrastructure).	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	24.2) Information security (including cyber security) requirements are included in the requirements defined for new information systems or enhancements to existing information systems.	< Maturity Level >		
	24.3) ICT security controls are implemented for all phases of the ICT solutions life cycle, starting from the design, development (incl. measures to protect the integrity of the source codes of ICT systems that are developed in-house), purchasing and testing phases and continuing through the operation phase.	< Maturity Level >		
	24.4) The ICT solutions life cycle standards, methodologies and safeguards also apply to End User Computing (EUC).	< Maturity Level >		
	Data quality management - Please note that this refers to risk, regulatory and financial reporting data		**Strengths**	**Weaknesses**
	Data quality management			
25	25.1) Data quality management procedures, are defined, documented and tested.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	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: (i) issuing policies and guidelines; (ii) overseeing proper implementation of the data governance and quality framework throughout the organisation; (iii) ensuring the evaluation and monitoring of data quality through data quality processes; and (iv) participating in relevant change management processes (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).	< Maturity Level >		
	25.3) The supervised entity's human and technical resources are sufficient to support an adequate level of data quality.	< Maturity Level >		
	25.4) Data quality management procedures include proper 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.). Please give details on the data quality tools/mechanisms adopted to support data quality management in Explanation, if any.	< Maturity Level >		
	25.5) 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 >		
	25.6) Data quality management procedures also apply to End User Computing (EUC).	< Maturity Level >		
	25.7) The resolution processes of critical data quality issues are documented.	< Maturity Level >		
	Data architecture model			
26	26.1) The supervised entity has defined and documented its data architecture, data models and data flows, and validated them with relevant business and ICT stakeholders.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope.	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope.
	26.2) The data architecture is regularly reviewed (and updated if needed).	< Maturity Level >		

	Questions to the ICT Risk Control Framework	Maturity levels	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	
26	26.3) Single golden (authoritative) sources are defined per risk category for data aggregation purposes.	< Maturity Level >	In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	26.4) The data architecture model includes data taxonomies / dictionary of the main business concepts and a metadata repository, which cover all material legal entities, business lines, material risks and material risk indicators, reports, and models.	< Maturity Level >		
	ICT continuity management		**Strengths**	**Weaknesses**
	Business impact analysis			
27	27.1) As part of the overall business continuity policy, the supervised entity conducts business impact analyses (BIA) of its exposures to severe business disruptions. Under the BIA, the supervised entity assesses 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.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented
	27.2) The supervised entity ensures 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 business continuity policy and planning			
28	28.1) As part of the ICT risk management framework referred to in Article 6(1) of Regulation (EU) 2022/2554 and based on the identification requirements set out in Article 8 of Regulation (EU) 2022/2554, the supervised entity has 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.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	28.2) The supervised entity includes in the ICT business continuity policy a description of all of the following: (i) the objectives of the ICT business continuity policy, including the interrelation of ICT and overall business continuity, and considering the results of the business impact analysis (BIA); (ii) the scope of the ICT business continuity arrangements, plans, procedures, and mechanisms, including limitations and exclusions; (iii) the timeframe to be covered by the ICT business continuity arrangements, plans, procedures, and mechanisms; (iv) the criteria to activate and deactivate ICT business continuity plans, ICT response and recovery plans, and crisis communications plans.	< Maturity Level >		
	28.3) The supervised entity includes in the ICT business continuity policy provisions on: (i) the governance and organisation to implement the ICT business continuity policy, including roles, responsibilities and escalation procedures ensuring that sufficient resources are available; (ii) the alignment of the ICT business continuity policy to the communication policy referred to in Article 14(2) of Regulation (EU) 2022/2554, and to the communication and crisis communication actions referred to in Article 11(2)(e), of Regulation (EU) 2022/2554.	< Maturity Level >		
	28.4) The supervised entity includes in the ICT business continuity policy provisions on: (i) 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, and concerning recovery objectives, specifying that the financial entity 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; (ii) the development of ICT business continuity plans for severe business disruptions as part of those plans, and the prioritisation of ICT business continuity actions using a risk-based approach.	< Maturity Level >		
	28.5) The supervised entity includes in the ICT business continuity policy provisions on: (i) 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; (ii) the review of the effectiveness of the implemented ICT business continuity arrangements, plans, procedures and mechanisms, in accordance with Article 26 of the RTS on ICT risk management.	< Maturity Level >		
	28.6) The supervised entity has implemented the ICT business continuity policy through dedicated, appropriate and documented arrangements, plans, procedures and mechanisms aiming to: (a) ensure the continuity of the financial entity's critical or important functions; (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; (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 of Regulation (EU) 2022/2554; (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 in accordance with Article 14 of Regulation (EU) 2022/2554, and report to the competent authorities in accordance with Article 19 of Regulation (EU) 2022/2554.	< Maturity Level >		
	28.7) As part of the ICT risk management framework referred to in Article 6(1) of Regulation (EU) 2022/2554, the supervised entity has implemented associated ICT response and recovery plans which are subject to independent internal audit reviews.	< Maturity Level >		

	Questions to the ICT Risk Control Framework	Maturity levels	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	
	28.8) The supervised entity has in place, maintains and periodically tests appropriate ICT business continuity plans, notably with regard to critical or important functions outsourced or contracted through arrangements with ICT third-party service providers.	< Maturity Level >		
	28.9) When developing the ICT response and recovery plans referred to in Article 11(3) of Regulation (EU) 2022/2554, the supervised entity takes into account the results of its business impact analysis (BIA). Those ICT response and recovery plans: (a) specify 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 financial entity; (c) are designed to meet the recovery objectives of the operations of the financial entities; (d) are 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) lay down the objectives of ICT response and recovery plans and the conditions to declare a successful execution of those plans.	< Maturity Level >		
	28.10) The ICT response and recovery plans identify relevant scenarios, including scenarios of severe business disruptions and increased likelihood of occurrence of disruption. Those plans develop scenarios based on current information on threats and on lessons learned from previous occurrences of business disruptions. The supervised entity duly takes into account all of the following scenarios: (a) cyber-attacks and switchovers between the primary ICT infrastructure and the redundant capacity, backups, and redundant facilities; (b) scenarios in which the quality of the provision of a critical or important function deteriorates to an unacceptable level or fails, and duly consider the potential impact of the insolvency, or other failures, of any relevant ICT third-party service provider; (c) partial or total failure of premises, including office and business premises, and data centres; (d) substantial failure of ICT assets or of the communication infrastructure; (e) the non-availability of a critical number of staff or staff members in charge of guaranteeing the continuity of operations; (f) impact of climate change and environment degradation related events, natural disasters, pandemics, and physical attacks, including intrusions and terrorist attacks; (g) insider attacks; (h) political and social instability, including, where relevant, in the ICT third-party service provider's jurisdiction and the location where the data are stored and processed; (i) widespread power outages.	< Maturity Level >		
	28.11) Where the primary recovery measures may not be feasible in the short term because of costs, risks, logistics, or unforeseen circumstances, the ICT response and recovery plans referred to in Article 26(1) of the RTS on ICT risk management framework consider alternative options.	< Maturity Level >		
	28.12) As part of the ICT response and recovery plans referred to in Article 26(1) of the RTS on ICT risk management framework, the supervised entity considers and implements continuity measures to mitigate failures of ICT third-party service providers of ICT services supporting critical or important functions.	< Maturity Level >		
	ICT business continuity testing and review			
	29.1) As part of its comprehensive ICT risk management, the supervised entity tests 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. These tests include 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 of Regulation (EU) 2022/2554.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	29.2) When testing the ICT business continuity plans in accordance with Article 11(6) of Regulation (EU) 2022/2554, the supervised entity takes into account the financial entity's business impact analysis (BIA) and the ICT risk assessment referred to in Article 3(1)(b) of the RTS on ICT risk management framework, and documents the results of the testing. Any identified deficiencies resulting from that testing are analysed, addressed, and reported to the management body.	< Maturity Level >		
29	29.3) The supervised entity assesses through the testing of its ICT business continuity plans whether ICT is able to ensure the continuity of the supervised entity's critical or important functions. That testing: (a) is performed on the basis of test scenarios that simulate potential disruptions, including an adequate set of severe but plausible scenarios, and including the scenarios considered for the development of the business continuity plans; (b) contains the testing of ICT services provided by ICT third-party service providers, duly considering scenarios linked to insolvency or failures of the ICT third-party service providers or linked to political risks in the ICT third-party service providers' jurisdictions, where relevant; (c) contains scenarios of switchover from primary ICT infrastructure to the redundant capacity, backups and redundant facilities, verifying whether at least critical or important functions can be operated appropriately for a sufficient period of time, and whether the normal functioning may be restored; (d) is designed to challenge the assumptions on which the business continuity plans are based, including governance arrangements and crisis communication plans; (e) contains procedures to verify the ability of the supervised entity'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 >		
	29.4) As part of its comprehensive ICT risk management, the supervised entity tests the crisis communication plans established in accordance with Article 14 of Regulation (EU) 2022/2554.	< Maturity Level >		

	Questions to the ICT Risk Control Framework	Maturity levels	Explanations Please indicate here strengths and weaknesses leading to the self-assessment score as well as explanations if the score deviates from last year's.	
	29.5) The supervised entity 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.	< Maturity Level >		
	29.6) The supervised entity 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.	< Maturity Level >		
	Crisis management and communication plans			
30	30.1) The supervised entity has implemented a crisis management function, which, in the event of activation of the ICT business continuity plans or ICT response and recovery plans, inter alia, sets out clear procedures to manage internal and external crisis communications in accordance with Article 14 of Regulation (EU) 2022/2554.	< Maturity Level >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	< Please explain why you chose the respective overall maturity level. If there are important variations within the entities in scope of the report, please make this clear and explain the nature of the variations. In case an assessment criteria has not been fully implemented for all the entities in scope, please mention any projects or initiatives that have been set up to improve the situation of the entities in scope. In case an assessment criteria has been fully implemented for all the entities in scope the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	30.2) As part of the ICT risk management framework referred to in Article 6(1) of Regulation (EU) 2022/2554, the supervised entity 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.	< Maturity Level >		
	30.3) As part of the ICT risk management framework, the supervised entity has implemented 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.	< Maturity Level >		
	30.4) At least one person in the supervised entity is tasked with implementing the communication strategy for ICT- related incidents and fulfil the public and media function for that purpose.	< Maturity Level >		

Gross costs and losses and financial recoveries in line with Regulation (EU) 2022/2554 (DORA) Article 11(10) and the EBA Joint Guidelines on estimation of aggregated annual costs and losses caused by major ICT-related incidents				
Reference year (e.g. 2025)	< Reference year >			
Accounting vs Calendar year	< Accounting year/Calendar year >			
Reference period (e.g Jan-Dec meaning 01/01-31/12)	< Reference period >			
Comments				
		Total for the reference year	< Total gross costs and losses >	< Total recoveries >

Number of incident	Date of the submission of the final incident report	Incident reference number	Gross costs and losses of the incident in the reference year (1000s of units)	Recoveries of the incident in the reference year (1000s of units)
1				
2				
3				
4				
5				

Information-sharing arrangements in line with Article 45 of Regulation (EU) 2022/2554			
Name	**Date of validation of membership**	**Date of cessation of membership**	**Scope of information exchange**

ICT Risk Level Guidance

Risk Level →	1 (Lowest exposure)	2	3	4 (Highest exposure)	COMMENT	RISK DEFINITION (EBA-GL-2017-05)
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 on-site inspections, internal audits as well as any other relevant reviews.*					
ICT security risk	The supervised entity would suffer no/negligible impact in the event of unauthorized access because it does not hold sensitive data on its ICT systems. Additionally, the supervised entity has encountered no incidents, no data breaches, and no critical findings.	The supervised entity would suffer limited impact in case of unauthorized access because it holds limited sensitive data on its ICT systems. Additionally, the supervised entity has encountered very low number of incidents and negligible losses due to data breaches.	The supervised entity would suffer medium impact in case of unauthorized access because of sensitive data on its ICT systems.	The supervised entity 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*	The risk of unauthorised access to ICT systems and data from within or outside the supervised entity (e.g. cyber-attacks).
ICT availability and continuity risk	The supervised entity would suffer no impact if ICT systems were to be unavailable for an extended period. Additionally, the supervised entity has encountered no loss due to unplanned downtime of critical systems, and there are no critical findings.	The supervised entity would suffer limited impact if ICT systems were to be unavailable for an extended period Additionally, the supervised entity has encountered negligible losses and a negligible number of hours of unplanned downtime.	The supervised entity would suffer medium impact if ICT systems were to be unavailable for an extended period.	The supervised entity 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 supervised entity's services, due to a failure of ICT hardware or software components; weaknesses in ICT system management; or any other event.
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 supervised entity to manage ICT system changes in a timely and controlled manner, in particular for large and complex change programmes.
ICT data integrity risk	Golden sources of data are defined to cover all critical or important functions. Additionally, the supervised entity has not encountered any cases of invalid data modification or of incorrect supervisory reporting data submitted. There are no critical findings.	Golden 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 Golden sources have been defined but sensitive data are still replicated within different bases and can be modified.	No Golden sources have been defined. Databases are fed with information manually.	*A Golden 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 supervised entity to provide services and produce (risk) management and financial information in a correct and timely manner.

ICT Risk Control Guidance

Criteria to consider →	A	B	C	D	E	F	G	H	I	J	
Maturity Level ↓	ICT risk controls should be assessed by how effectively they mitigate ICT risks including any reflection on this effectiveness based on investigation results of for example on-site inspections, internal audits and other such exercises.										**Summary (see below for more detail on criteria)**
1 (Best controls in place)	✓	✓	✓	✓	✓						Controls in place are very mature and well established. 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. There is some potential for improvement/ optimisation.
3	✓	✓	✓				✓	✓			Some controls are in place, but they are not consistent across the entire organisation and locations. 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.

A - Documented: Controls and processes are documented and have a documented control owner.

B - Tested: Controls are tested on a regular basis: controls are formally tested by management and internal audit.

C - Reviewed: Controls are reviewed as part of scheduled Risk assessment and updated accordingly.

D - Operating effectively as part of Business As Usual (BAU): Controls are fully implemented and operating effectively, based on independent testing.

E - Optimised: Controls reflect best practice, are automated where possible, are operating effectively based on consecutive past audits, and are reviewed periodically and improved where feasible.

F - Improved: Through testing and review, control improvements have been identified and implemented.

G - Implementation Underway: Controls are documented, tested and reviewed, but are not operating effectively. Some process and control improvement projects are

H - Control not operating effectively: Controls are documented, tested and reviewed, but are not operating effectively in at least one instance/ location/ legal entity.

I - Investment/ Project Underway: Controls are not in place (not documented, tested, reviewed and operating) for this specific control area and/ or a Project is Underway to implement/ re-engineer processes and controls and it will take time for these controls to become embedded as part of BAU.

J - Control not in place: Control is not documented, implemented, operating, tested or reviewed.

Term	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 ICT System	The criticality of an ICT system should be based on how it supports the bank's critical or important functions as well as how a disruption of the system would impact business processes and activities of the bank.	
Cyber alert	1. Notification that a specific cyber incident has occurred or a cyber threat has been directed at an organisation's information systems. Source: Adapted from NIST 2. Announcement of an abnormal situation or condition (from one or more cyber events) requiring attention. Source: Adapted from ISO 8468 2007	FSB Cyber Lexicon (as updated in 2023), https://www.fsb.org/wp-content/uploads/P130423-3.pdf, NIST, ISO 8468 2007
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 know as EUDA - End User Developed Application.	COBIT
Financials	The Financials section of the General Data sheet should be closely aligned to the FINREP reporting of the SIs and normally be reported on a P&L basis. We would also kindly ask to describe any potential differences in the explanation column.	
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.	
Golden source	A single authoritative source for risk data per each type of risk in order to generate accurate and reliable risk data to meet normal and stress/crisis reporting accuracy requirements. Data should be aggregated on a largely automated basis so as to minimise the probability of errors. Golden sources mean data which can be trusted because they are well-defined, complete and accurate information. Front-office or back office ICT applications where exposures and positions are managed, but more often the accounting system is recognised as a golden source	BCBS 239
Gross costs and losses and financial recoveries	As specified in the EBA Joint Guidelines on estimation of aggregated annual costs and losses caused by major ICT-related incidents (https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/operational-resilience/joint-guidelines-estimation-aggregated-annual-costs-and-losses-caused-major-ict-related-incidents)	EBA Joint Guidelines on estimation of aggregated annual costs and losses caused by major ICT-related incidents
IAM (Identity Access Management)	Encapsulates people, processes and technology to identify and manage the data used in an information system to authenticate users and grant or deny access rights to data and system resources.	FSB Cyber Lexicon (as updated in 2023), https://www.fsb.org/wp-content/uploads/P130423-3.pdf, NIST, ISO 8468 2007
ICT budget	Estimated costs for the functioning and the development of the ICT, covering both 'run' ICT, meaning the ongoing costs of operating and maintaining the current ICT systems and services, and 'change' meaning the development and the implementation of new ICT systems (business application and ICT infrastructure) and services , including the enterprise's portfolio of ICT-enabled investment programmes An ICT budget should be segmented to include the following: support /maintenance of the ICT environment, network and infrastructure, hardware, software, cloud services, backup, disaster recovery and business continuity, projects, miscellaneous/ICT emergencies.	
ICT resilience	ICT (and cybersecurity resilience) mean the ability to protect, detect, respond and recover in order to support and facilitate the delivery of critical operations.	BCBS Principles for Operational Resilience, March 2021
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 supplier or by an ICT third-party service provider, but that is still in use and supports the functions of the financial entity	Regulation (EU) 2022/2554 (DORA) Article 3(3)
Malware (malicious software)	Any program or file that is harmful to a computer user, which includes computer viruses, worms, Trojan horses and spyware.Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems.	FSB Cyber Lexicon (as updated in 2023), https://www.fsb.org/wp-content/uploads/P130423-3.pdf, NIST, ISO 8468 2007
MTPD (maximum tolerable period of disruption)	The maximum tolerable period of disruption (MTPD) of a process designates the time frame in which the process must be recovered so that the organisation does not enter a phase in which their ability to survive is threatened in the short-term or long-term.	BSI-Standard 100-4
Physical security expenses	Physical security encompasses all measures to protect premises/datacenters from intrusion and destruction (e.g. fire, flood, earthquake, etc.). For instance physical security budget covers: video surveillance, fire/smoke/temperature/humidity sensors, physical access control, automated extinguisher system, air conditioning, secured doors/windows, safes to store backup supports & documents, etc.	
RPO (recovery point objective)	Point to which data must be restored to enable the activity to operate on resumption.	ISO 22301:2012

Term	Definition	Source
RTO (recovery time objective)	The recovery time objective (RTO) specifies the time in which the process is intended to be recovered. The time frame specified for the RTO must be lower than the maximum tolerable period of disruption MTPD.	BSI-Standard 100-4
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 event	An occurrence (e.g., an auditable event or flag) considered to have potential security implications to the system or its environment that may require further action (noting, investigating, or reacting), such as for example physical or logical intrusion as well as breaches of confidentiality, integrity and availability of the information assets	NIST
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	FSB Cyber Lexicon (as updated in 2023), https://www.fsb.org/wp-content/uploads/P130423-3.pdf, NIST, ISO 8468 2007
SSM Countries	All euro area countries participate automatically in the SSM. A list of all EU member using the euro is available at hhttps://www.bankingsupervision.europa.eu/about/thessm/html/index.en.html	Euro area
Supervised Entity	Used in line with the scope of the IT Risk Questionnaire and normally aligned with the prudential scope of consolidation. Differences should be indicated in the Entities in scope sheet.	
Supervisory Reporting	Supervisory reporting includes all the regular submission to the supervisor: COREP, FINREP, STE and STE-equivalent (as NPL reporting).	