EUROPEAN CENTRAL BANK
BANKING SUPERVISION

ECB-PUBLIC

IT Risk Questionnaire Publication (ITRQ) - 2022

Notice

The ECB has decided to publish, for transparency and accountability purposes, its 'Information Technology Risk Questionnaire' (ITRQ) 2022 covering the period from 1 January 2021 to 31 December 2021.

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). The ITRQ, forms an integral part of the risk assessment methodology which was developed by the ECB Banking supervision together with the National Competent Authorities and include thematic reviews, horizontal analyses on IT risk topics and a reporting framework for any significant cyber incidents affecting supervised credit institutions.

The questionnaire allows a standardised regular data collection from the 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 IT risk.

For more information about its structure and the risk categories reflected in it please see the ”Annual report on the outcome of the SREP IT Risk Questionnaire”.

Final Version: 11/11/2021

Reference year: 01/01/2021 to 31/12/2021

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 IT 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 28 February 2022.

Tabs	Comments	To be filled-in by the supervised entity	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 **36** questions designed to provide an **IT overview** of the supervised entity.	Answers	**0%**
		Explanations	**0%**
IT Risk Level Self-Assessment	IT Risk Level (ITRL) Self-Assessment encompasses 38 questions to self-assess the firm's **overall risk level** across **five areas**.	Answers	**0%**
		Explanations	**0%**
		Self-Assessments	**0%**
IT Risk Control Self-Assessment	IT Risk Control (ITRC) Self-Assessment comprises a series of closed (e.g. "yes/no") questions designed to self-assess the **maturity level** of **35 IT key controls** across 10 IT areas.	Answers	**0%**
		Explanations	**0%**
		Self-Assessments	**0%**
ITRL_Guidance	These **Guidance** tabs have been created to help selecting the self-assessment scores within the IT Risk Level (ITRL) and IT Risk Control (ITRC) tabs.		
ITRC_Guidance			
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 (1 January 2021 to 31 December 2021)

Optional column for Firm's internal use. Please note that the content of this column will not be considered by supervisors.

	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	Contact person(s) / Title(s)	< e.g. Peter Smith/Head of IT, Bank ABC; Anna Walter/CISO, Group XYZ >
5	Email address(es) of contact person(s)	< e.g. Smith: Peter.Smith@bankABC.com; Walter: Anna.Walter@groupxyz.com >
6	Telephone number of contact person(s)	< e.g. Smith: 0033 111 222 333; Walter: 0033 111 111 111) >

Details of the entity in scope

	Staff	Answers		Explanations Please provide further details here
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.*	< # 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) >
7a	Of which, number of employees (with individual permanent contract - FTEs) delivering IT services (including IT security and IT risk management) to the supervised entity (SE) in scope, as of 31.12 of reference year.	< # of Group **permanent** IT FTEs >	< Of which, # of SE **permanent** IT FTEs >	< i.e. permanent IT FTEs = staff members on **individual contract of indefinite duration** delivering IT services > < i.e. Group permanent IT FTEs = staff under individual contract with the group (both parent and subsidiaries/sub-entities including the SE) > < i.e. SE permanent IT FTEs = staff under individual contract directly with the SE >
7b	Of which, number of employees (with individual fixed-term contract - FTEs) delivering IT services (including IT security and IT risk management) to the supervised entity (SE) in scope, as of 31.12 of reference year.	< # of Group **non-permanent** IT FTEs >	< Of which, # of SE **non-permanent** IT FTEs >	< i.e. non-permanent IT FTEs = employees on i**ndividual fixed-term contract** delivering IT services > < i.e. Group non-permanent IT FTEs = employees under individual contract with the group (both parent and subsidiaries/sub-entities including the SE) > < i.e. SE non-permanent IT FTEs = employees under individual contract directly with the SE >
8	Personnel (e.g. consultants, technical support) provided by business partners, delivering IT services (including IT security and IT risk management) to the supervised entity (SE) in scope, as of 31.12 of reference year.	< # of Group **temporary** IT FTEs >	< # Of which SE **temporary** IT FTEs >	< i.e. temporary IT FTEs = personnel delivering IT services to the supervised entity **via non-individual contract** (e.g. provided by external IT companies, consultancy services) > < i.e. Group temporary IT FTEs = provider(s) under contract with a group entity distinct from the SE> < i.e. SE temporary IT FTEs = contract(s) with provider(s) signed directly by the SE >
9	Overall number of personnel located out of the SSM countries and providing IT services (employees of the SE/Group, personnel provided via extra-group companies)	< Total # of **non-SSM** IT FTEs >	< Of which, # of **non-SSM** permanent IT FTEs >	< Please indicate the FTEs (Full Time Equivalent) located outside the SSM countries and delivering IT services to 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.>
10	Number of locations of significant IT functions and data centres outside the SSM countries.	< # of IT 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**. >
11	Is there a functional independence between 1st and 2nd Line of Defence (LoD) in the IT risk area?	< Yes / No >	< Name of the function / committee to which the 2 LoD in IT area is reporting to >	< Please specify how the independence criteria are assured >
12	Number of vacant positions and percentage of staff turnover in the IT department for the reference year (IT staff leaving the entities in scope; including IT security, IT risk management and covering all IT functions)	< # of IT vacancies (including IT risk and IT/information security) >	< Average period (# of months) position remained vacant >	< Please provide information regarding how many positions (i.e. internal permanent staff) are vacant and details for critical IT positions, e.g. Head of IT, 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 IT departments is seen compared to the overall staff turnover for the entities in scope. >
		< % of IT staff turnover (including IT risk and IT/information security) >	< % of total staff turnover >	
13	Number of IT personnel within the 1st Line of Defence (LoD)	< # of IT 1st LoD FTEs >	< # of IT 1st LoD staff vacancies >	< 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. IT risk, IT operation, IT 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. >
		< % of IT 1st LoD staff turnover >	< Average period (# of months) position remained vacant >	
14	Number of IT Risk personnel within the 2nd Line of Defence (LoD)	< # of IT 2nd LoD FTEs >	< # of IT 2nd LoD staff vacancies >	< 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. IT risk, IT operation, IT security etc.). Please indicate and elaborate on IT 2LoD staff turnover, where staff turnover refers to the number or percentage of workers who leave the department and are replaced by new employees. >
		< % of IT 2nd LoD staff turnover >	< Average period (# of months) position remained vacant >	
15	Number of IT Auditor(s) within the 3rd Line of Defence (LoD)	< # of Local IT Audit FTEs >	< # of IT Audit staff vacancies >	< Please indicate the FTEs (Full Time Equivalent) employed by the supervised entities for this function. Please also detail where applicable, how many IT Audit staff have formal IT 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 IT Audit staff turnover, where staff turnover refers to the number or percentage of workers who leave the department and are replaced by new employees. >
		< % of IT Audit staff turnover >	< Average period (# of months) position remained vacant >	

	Financials (please refer to the Glossary for this section)	Answers			Explanations
16	Past (for the year before reference year) and future / forecast IT expenses of the supervised entity (SE) in scope of this report (1 total figure for complete scope, in EUR)	< Actual IT running expenses **for the year before** the reference year in € >	< Actual IT change expenses **for the year before** the reference year in € >		< e.g. IT expenses: 45,000,000 EUR, comprising extraordinary expenses of 10,000,000 EUR due to a major damage in data centre A of TechbankABC caused by flooding >
		< IT running expenses forecast **for the year after** the reference year in € >	< IT change expenses forecast **for the year after** the reference year in € >		
17	IT expenses of the supervised entity (SE) in scope of this report (in EUR) for the reference year	<IT running expenses for the reference year in €>	<IT change expenses for the reference year in €>		< e.g. Comprising 20,000,000 EUR for IT Operations; 10,000,000 EUR for IT Security Management; etc. IT outsourcing expenses are included in the IT expenses. >
17a	Of which, IT expenses related to the IT security areas of the supervised entity (SE) in the scope of this report.	< Overall IT Security expenses for the reference year in € >	< Overall budgeted IT Security expenses **for the year after** the reference year in € >		< e.g. Comprising 20,000,000.00 EUR for IT Operations; 10,000,000.00 EUR for IT Security Management; etc. > < Please indicate the 5 biggest contributors to the IT security expenses for the reference year regarding the coverage by topic (e.g. monitoring and detection, identity & access management, data leakage protection, etc.). >
		< Of which, Physical IT Security expenses for the reference year in € >	< Of which, budgeted physical IT Security expenses **for the year after** the reference year in € >		
17b	Of which, how much budget was spent on IT innovations in the reference year? (in EUR)	< e.g. €45000000 >			< Please describe in short your approach regarding the adaption of innovation and how this is reflected in your IT strategy. Innovative IT solutions could be peer-to-peer (P2P) lending, crowdfunding, robo advice, distributed ledger technologies, instant payment infrastructure, collateral optimisation services, etc. >
17c	Of which, IT outsourcing expenses in the reference year (in EUR).	< Of which IT Outsourcing Expenses in € (INTRA-group) >	< Of which IT Outsourcing Expenses in € (EXTRA-group) >		< Please explain and provide a breakdown of the 5 most relevant providers (external and cloud) with information about the related regular costs and the nature of the service delivered. e.g. The biggest outsourcing expenses external to Group for the entities in scope are IBM (10,000,000 EUR) and Microsoft (5,000,000.00 EUR). The biggest cloud computing expenses are Microsoft (2,000,000.00 EUR), which is a subset of the value indicated above. The biggest outsourcing expenses internal to Group are Group_ITOps (25,000,000 EUR) and Group_SOC (40,000,000 EUR) who provide shared IT services to Group entities. >
		< Of which **CLOUD** Expenses in € (INTRA-group) >	< Of which **CLOUD** Expenses in € (EXTRA-group) >		
18	IT outsourcing budget forecast for the year after the reference year (in EUR)	< IT Outsourcing Budget (INTRA-group) in € >	< IT Outsourcing Budget (EXTRA-group) 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 IT Operations services at techiA. >
19	Total amount of expenses (i.e. IT + non-IT) of the supervised entity (SE) in scope of this report (1 total figure for complete scope, in EUR)	< Budgeted Expenses (IT & non-IT) **for the year after** the reference year in € >			< e.g. Comprising 80,000,000 EUR for Payroll; 30,000,000.00 EUR Marketing; 100,000,000 EUR for acquisitions; etc. >
19a	Total outsourcing expenses (**IT & non-IT**) in the reference year (in EUR)	< Total Outsourcing Expenses in € >			< Please consider that total outsourcing also includes IT outsourcing. Please explain and include also INTRA-group outsourcing, along with information about the related regular costs and the nature of the service delivered. >
		< Of which Total Outsourcing Expenses in € (INTRA-group) >	<Of which Total Outsourcing Expenses in € (EXTRA-group) >		
20	Please list top 5 outsourcing providers in terms of volume of expenses (costs)	< Outsourcing provider >	< Type of outsourcing >	< Volume of expenses (costs) per outsourcer in € >	< Please provide main type of outsourcing services and/or areas to which outsourcing is related to. To be filled on a best effort basis. >
		< Outsourcing provider >	< Type of outsourcing >	< Volume of expenses (costs) per outsourcer in € >	< Please provide main type of outsourcing services and/or areas to which outsourcing is related to. To be filled on a best effort basis. >
		< Outsourcing provider >	< Type of outsourcing >	< Volume of expenses (costs) per outsourcer in € >	< Please provide main type of outsourcing services and/or areas to which outsourcing is related to. To be filled on a best effort basis. >
		< Outsourcing provider >	< Type of outsourcing >	< Volume of expenses (costs) per outsourcer in € >	< Please provide main type of outsourcing services and/or areas to which outsourcing is related to. To be filled on a best effort basis. >
		< Outsourcing provider >	< Type of outsourcing >	< Volume of expenses (costs) per outsourcer in € >	< Please provide main type of outsourcing services and/or areas to which outsourcing is related to. To be filled on a best effort basis. >
21	Please list top 5 IT outsourcing providers in terms of volume of expenses (costs)	< Outsourcing provider >	< Type of outsourcing >	< Volume of expenses (costs) per outsourcer in € >	< Please provide main type of IT outsourcing services and/or areas to which outsourcing is related to. To be filled on a best effort basis. >
		< Outsourcing provider >	< Type of outsourcing >	< Volume of expenses (costs) per outsourcer in € >	< Please provide main type of IT outsourcing services and/or areas to which outsourcing is related to. To be filled on a best effort basis. >
		< Outsourcing provider >	< Type of outsourcing >	< Volume of expenses (costs) per outsourcer in € >	< Please provide main type of IT outsourcing services and/or areas to which outsourcing is related to. To be filled on a best effort basis. >
		< Outsourcing provider >	< Type of outsourcing >	< Volume of expenses (costs) per outsourcer in € >	< Please provide main type of IT outsourcing services and/or areas to which outsourcing is related to. To be filled on a best effort basis. >
		< Outsourcing provider >	< Type of outsourcing >	< Volume of expenses (costs) per outsourcer in € >	< Please provide main type of IT outsourcing services and/or areas to which outsourcing is related to. To be filled on a best effort basis. >

	Oversight	Answers			Explanations
22	How many Board members of the supervised entity (SE) in the scope of this report have IT expertise (e.g. IT qualification and/or IT certification)?	< Avg # of Board members with IT expertise per SE >	< Avg # CIO as Board members (i.e. CIO as dedicated reference) per SE >	< Avg # of Board members per SE >	< Average number of Board Members with IT expertise on the Boards of the supervised entities calculated across the boards - e.g. to qualify, a Board member would be expected to hold a recognised qualification in an IT discipline (e.g. Certified Associate in Project Management (CAPM), Certified in the Governance of Enterprise IT (CGEIT), Certified Scrum Master (CSM), Certified Information Systems Security Professional (CISSP), COBIT 5 Foundation Certification, CompTIA Project+, Information Technology Infrastructure Library (ITIL), PMI Agile Certified Practitioner (PMI-ACP), Six Sigma Certification, TOGAF 9 Certification or similar certificates) and/or have held a position requiring significant IT knowledge.>
23	How often is IT, including Information Security, part of the agenda of the management board and formally discussed?	< select Frequency category >			< e.g. Formally discussed IT matters should be officially recorded in the minutes of the board meeting >
24	Indicate the frequency of oversight of IT outsourced services (e.g. KPI reviews, including remediation actions and associated timeframes, discussions of IT Risks at senior management / board level)	< Frequency of KPI reviews >	< Frequency of discussion on IT Outsourcing 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 IT Outsourcing risks should be officially recorded in the minutes of board meetings. >
25	Is there a process that ensures that IT strategies and governance documents defined at group level are tailored to comply with local regulations and operational constraints? Where Yes, please provide details on the how in the column "Explanations".	< Yes / No >			< Please provide details. >
26	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?	< 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. >
27	Internal IT 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.*	< # of IT Audits in reference year >			< Please provide details of the most critical IT Audit issues/findings and, if any, expose reasons for excluding IT functions from the scope of IT Audits. Please provide a list of the IT audits (either internal or external) performed in the last three years where the most critical findings were detected. Please specify whether the internal IT Audit Unit is in charge of the monitoring / follow up of the remediation actions of SSM or other external IT 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 IT risk related topics. >
		< Total # of IT findings identified in reference year >	< Total # of IT findings closed in reference year >	<Total # of IT findings currently outstanding>	
		< Of which # of critical IT findings identified in reference year >	< Of which # of critical IT findings closed in reference year >	< Of which # of critical IT findings currently outstanding>	< Please provide details related to the overall IT audit issues/findings and critical where indicated. Please specify how many of the current outstanding critical IT findings are open since a year or more. >
		< Average duration (# in months) to close critical IT finding >			
		< Total # of overdue IT findings >	< Main type of overdue IT findings >		
		< Of which # of overdue critical IT findings >	< Main type of overdue critical IT findings >		
28	External IT 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)	< Total # of external IT findings identified in reference year >	< Of which # of external critical IT findings identified in reference year >		< Please provide details related to the external IT audit issues/findings and critical ones. >
29	Percentage of IT functions within the scope of this report NOT assessed by Internal Audit (IA) (including outsourced IT functions)	< % of IT functions NOT reviewed by Internal Audit within the ref. year >	< % of IT 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 IT functions not covered, please include outsourced IT functions. This information may have been presented to the Audit Committee as % of IT Audit Universe not covered. >
		< % of IT Outsourcing functions NOT reviewed by Internal Audit within the ref. year>	< % of IT Outsourcing functions NOT reviewed by Internal Audit in the reference year and preceding 2 years >		

	IT Environment	Answers			Explanations
30	Have there been any mergers, acquisitions, carve outs or other major organisational changes leading to merging or splitting of IT 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 IT landscape in the reference year. >
31	Number of critical projects with significant IT undertaking involved, planned/in progress/completed in the reference year	< Total # of projects >	< Related expenses in € >		< If any, please provide name, description, projected and actual budget in €, start and projected end date, current status. >
31a	Of which, number of critical projects with impact on the IT landscape/architecture	< 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 IT architecture. >
31b	Of which, number of projects related to end-of-life (EOL) systems (replacement or mitigation)	< Of which, # of projects related to EOL 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 mitgation of EOL systems). >
32	What was the total number of successful cyber-attacks (including those aiming at outsourced service providers) in the reference year?	< # 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.). >
		< Average time for detection (all type of cyber-attacks - in hours) >	< Average time for recovery (all type of cyber-attacks - in hours) >		
		< Average time for detection (cyber-attacks excluding DDOS - in hours) >	< Average time for recovery (cyber-attacks excluding DDOS - in hours) >		
33	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 EUR)?	< 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. >
34	How many incidents were reported to the supervisor according to the SSM Cyber Incident Reporting Framework in the reference year? What was the total amount of direct and indirect costs? (for the entities in scope)	< # of incidents reported to the supervisor >	< Total losses due to incidents reported to the supervisor in € >		< Please briefly explain the main root causes for the incidents caused by cyber-attacks. In case there is a gap between internally reported incidents caused by cyber-attacks and the ones submitted to the supervisor, please explain. >
35	Does the supervised entity (SE) in the scope of this report have insurance contracts covering cyber-risk?	< 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 IT risk covered and/or not covered. Please briefly explain calculation of the direct and indirect costs. >
36	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?	< Yes / No >	< Number of on-going projects related to "innovation" >	< Of which number 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 >

	General comments

	Questions to the IT Risk Level of the entities in scope Unless specified otherwise, the question shall be answered in relation to the reference year (1 January 2021 to 31 December 2021)	**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.	**Overall IT Risk Level Self-Assessment**	**Optional column for Firm's internal use.** Please note that the content of this column will not be considered by supervisors.
	IT security risk				
1	How many external companies (all that are different from the supervised entities assessed) have any kind of access to internal systems? (as of 31.12 of reference year)	< e.g. 30 firms >	< 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. >	< 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?	< e.g. 2 data breach incidents >	< 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. >		
3	Number of no longer supported (i.e. out of support without extended support agreement) end-of-life (EOL) systems (such as operating systems, databases systems, network systems, underlying software) that support critical processes. (as of 31.12 of reference year)	< e.g. number of EOL systems >	< Please specify which business critical processes are dependent on end-of-life (EOL) systems and to which extent. Please indicate which system is end-of-life (EOL) (if there are too many indicate the total number); which projects are in place aiming at migrating the EOL systems and their associated completion deadlines. >		
3a	Of which, how many end-of-life (EOL) systems are planned to be replaced within next year (i.e. a concrete project for the EOL system replacement which is at least planned and approved)?	< e.g. number of EOL to be replaced >	< Please specify which end-of-life (EOL) systems are going to be replaced within next year, which projects are in place aiming at migrating the EOL systems and their associated completion deadlines. >		
3b	Of which, for how many end-of-life (EOL) 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?	< e.g. number of EOL with migration plan >	< Please specify in case there are no migration plans. Please specify type of end-of-life (EOL) and how many there are per type in %. >		
4	Number of no longer supported end-of-life (EOL) systems (such as operating systems, databases systems, network systems, underlying software) that are connected to any external networks. (as of 31.12 of reference year)	< e.g. number of EOL systems >	< Please specify which end-of-life (EOL) systems are connected to the external network. Please specify the type of EOL and how many they are per type in %. >		
5	Number of instances of end-of-life (EOL) systems (e.g. laptops/workstations still running under Windows XP)	< e.g. number of EOL impacted instances >	< Please specify the number of instances per each type of end-of-life (EOL) system. Please specify the % of affected instances overall total instances per each type of EOL system. >		
6	How many breaches of confidentiality (unauthorised access to data) were caused by security incidents (including cyber-attacks) in the reference year?	< e.g. 4 data breach incidents >	< 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. >		
6a	For the breaches of confidentiality caused by security incidents, please specify average detection time, in hours (i.e. time to detect the incident).	< e.g. 4 hours >	< Please specify the shortest and longest detection times of security incidents and how how they were detected. >		
6b	For the breaches of confidentiality caused by security incidents, please specify average recovery (resolution) time, in hours.	< e.g. 4 hours >	< Please specify the shortest and longest recovery times of security incidents and how many FTEs were involved. >		
7	How many remediation actions to mitigate IT 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 IT assets, it can be considered only once.	< e.g. 15 actions >	< Please specify which remediation actions are delayed by more than 1 year and initiatives planned to remediate IT security vulnerabilities lasting longer than 1 year. Please note that vulnerabilities of all criticality levels are in scope.>		
7a	Of which, the number of remediation actions to mitigate IT security vulnerabilities (e.g. identified by penetration tests or vulnerability scanning) that are overdue (as of 31.12 of reference year)	< e.g. 15 actions >	< Please specify which remediation actions are overdue, the main rationale and initiatives planned to remediate it. >		
8	How many critical audit, on-site inspection and internal model investigation findings related to IT security risk have not been remediated for longer than 1 year? (as of 31.12 of reference year)	< e.g. 15 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. >		
	IT availability and continuity risk				
9	How many different locations or data centres (including IT recovery sites) supporting/hosting business critical activities exist for the entities in scope? (as of 31.12 of reference year)	< e.g. 20 locations >	< Please describe what you consider as a business critical IT operations/data centre. Please list the locations of business critical IT operations/data centres. - e.g. Frankfurt - 2; London - 4; New York - 4; etc. Please clarify your definition of "critical". >	< Select Overall Risk Level >	
9a	Of which: the number of outsourced data centres supporting/hosting critical activities?	< e.g. 20 locations >	< Please specify the number of data centres supporting/hosting critical activities which are operated by third party service providers. >		
10	How many times were the IT continuity and disaster recovery (DRP) plans triggered during the reference year? (Continuity tests and exercises are not in scope)	< e.g. 5 times >	< Please include reference to the date and short description of the reasons. Please list only real situations not regular testing. >		
11	How many times has the crisis incident response team been activated (excluding exercises) during the reference year?	< e.g. 5 times >	< Please include reference to the date and short description of the reasons. Please list only real situations not regular testing. >		
12	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 entities 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). >		
13	Does the entity in scope provide critical 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 services offered to other institutions and your approximate market share in this service in SSM countries. >		
14	What was the overall unplanned downtime (in hours) of critical IT 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.	< e.g. 9 hours >	< Please mention the most significant downtimes of critical IT systems and the main root causes for these downtimes. Please use the definition of "Critical System" outlined in the Glossary tab or clarify your definition of "critical". 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) >		
14a	Of which, the overall unplanned downtime (in hours) that exceeded business agreements (e.g. SLA, RTO)?	< e.g. 9 hours >	< Please specify the total duration of downtimes of critical IT systems in excess of business agreements (corresponding to question #15a). >		
15	What was the overall number of unplanned downtimes of critical IT systems in the reference year (incl. those caused by external service providers)?	< e.g. number of unplanned downtimes >	< Please report the number of downtimes of critical IT systems (corresponding to question #14). >		
15a	Of which, the number of unplanned downtimes that exceeded business agreements (e.g. SLA, RTO)	< e.g. number of unplanned downtimes exceeding business agreements >	< Please specify how many downtimes exceeded business agreements. Please specify the main root causes for these downtimes. >		
16	What was the amount of losses (direct and indirect) due to the disruption of critical IT systems (incl. those caused by external service providers) and with material impact to customers in the reference year (in EUR)?	< e.g. €20000000 >	< Please mention the major loss drivers. Please use the definition of "Critical System" outlined in the Glossary tab or clarify your definition of "critical". >		
17	What was the overall unplanned downtime (in hours) of material customer service due to IT disruptions in the reference year? Where applicable, please provide a breakdown of any outage by service, frequency and duration(s) in the Explanation section.	< e.g. 17 hours >	< 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) >		
18	What was the overall number of unplanned downtimes of material customer service due to IT disruptions in the reference year?	< e.g. number of unplanned downtimes >	< Please specify the number of unplanned downtimes of material customer services (corresponding to question #17). >		
19	How many critical audit, on-site inspection and internal model investigation findings related to IT availability and continuity risk have not been remediated for longer than 1 year? (as of 31.12 of reference year)	< e.g. 15 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 of when the remediation actions will be completed. >		

	Questions to the IT Risk Level of the entities in scope Unless specified otherwise, the question shall be answered in relation to the reference year (1 January 2021 to 31 December 2021)	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.	Overall IT Risk Level Self-Assessment
	IT change risk			
20	How would you describe the overall complexity of the IT 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)	< select IT complexity >	< Please explain what kind of existing complexity is or might become an issue for the entities in scope and what is planned to reduce this complexity. >	< Select Overall Risk Level >
21	What is the number of IT systems (such as operating systems, databases systems, network systems, underlying software, excluding hardware, ATMs, mobile devices, etc.) for the entities in scope? (as of 31.12 of reference year)	< e.g. 1000 IT systems >	< What is considered to be an IT system is defined in the EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP), also outlined in the Glossary tab. Please mention the calculation view.>	
21a	Of which, number of IT systems supporting critical processes for the entities in scope? (as of 31.12 of reference year)	< e.g. 500 critical IT systems >	< What is considered to be a critical IT system is defined in the EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP), also outlined in the Glossary tab, or clarify your definition of "critical". Please mention the 5 most critical systems of the entities in scope. >	
21b	What is the number of instances of IT systems for the entities in scope? (as of 31.12 of reference year)	< e.g. 10000 instances >	< What is considered to be an IT system is defined in the EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP), also outlined in the Glossary tab. >	
22	How many changes in IT production environments hosting critical IT systems (e.g. networks, infrastructures, critical applications and technologies supporting major business products or services) were conducted in the reference year?	< e.g. 400 changes >	< 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". >	
22a	Of which, number of changes classified as "emergency changes"	< e.g. 400 changes >	< 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'. >	
22b	Of which, number of changes that caused issues	< e.g. 76 changes lead to issues >	< 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 >	
23	How many critical audit, on-site inspection and internal model investigation findings related to IT change risk have not been remediated for longer than 1 year? (as of 31.12 of reference year)	< e.g. 6 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". >	
	IT outsourcing risk			
24	How relevant are outsourced IT services (intra- and extra-group) for critical activities in IT operations, IT development or IT security? (as of 31.12 of reference year) *Please refer to the glossary for a definition of intra and extra group outsourcing*	< i.e. 1. Fully outsourced, 2. Largely outsourced, 3. Partially outsourced, 4. All in-house >	< Please specify which critical activities in IT operations, IT development or IT security have been outsourced to which major IT service providers. Please refer to the glossary for a definition of intra and extra group outsourcing. >	< Select Overall Risk Level >
24a	How relevant are outsourced IT services for critical activities in IT operations, IT development or IT security via INTRA-group outsourcing? (as of 31.12 of reference year)	<i.e. 1. Full intra-group outsourcing, 2. Largely intra-group outsourcing, 3. Partial intra-group outsourcing, 4. No intra-group outsourcing >	< Please specify which critical activities in IT operations, IT development or IT security have been outsourced to which major intra-group IT service providers (where intra-group are outsourcing arrangements provided by an entity belonging to the same corporate group. Please refer to the glossary for a definition of intra and extra group outsourcing. To be filled-in on a best effort basis. In providing the response, please give the view of the Supervised Entity which is consolidating this questionnaire (e.g. HQ entity for SSM-based banking groups, or main ECB supervised entity for banking groups headquartered outside of SSM countries). >	
24b	How relevant are outsourced IT services for critical activities in IT operations, IT development or IT security via EXTRA-group outsourcing? (as of 31.12 of reference year)	<i.e.1. Full extra-group outsourcing, 2. Largely extra-group outsourcing, 3. Partial extra-group outsourcing, 4. No extra-group outsourcing >	< Please specify which critical activities in IT operations, IT development or IT security have been outsourced to which major extra-group IT service providers (extra-group are outsourcing arrangements provided by entities outside the corporate group). Please refer to the glossary for a definition of intra and extra group outsourcing. To be filled-in on a best effort basis. In providing the response, please give the view of the Supervised Entity which is consolidating this questionnaire (e.g. HQ entity for SSM-based banking groups, or main ECB supervised entity for banking groups headquartered outside of SSM countries). >	
25	What is the largest percentage of value of EXTRA-group outsourcing contracts for IT services provided by a single external service provider divided by total value of all outsourced IT services EXTRA-group outsourcing? (as of 31.12 of reference year)	< e.g. 60 % >	< Please name your largest IT service provider and the nature of IT services outsourced to this extra-group provider (where intra-group are outsourcing arrangements provided by an entity belonging to the same corporate group; extra-group are outsourcing arrangements provided by entities outside the corporate group). To be filled-in on a best effort basis. >	
26	What is the largest percentage of value of INTRA-group outsourcing contracts for IT services provided by a single intra-group service provider divided by total value of all outsourced IT services for INTRA-group outsourcing? (as of 31.12 of reference year)	< e.g. 60 % >	< Please name your largest IT service provider and the nature of IT services outsourced to this intra-group provider (where intra-group are outsourcing arrangements provided by an entity belonging to the same corporate group; extra-group are outsourcing arrangements provided by entities outside the corporate group). To be filled-in on a best effort basis. >	
27	What is the overall number of outsourcing contracts, both INTRA-group and EXTRA-group?	< e.g. # of outsourcing contracts >	< Please briefly describe main types of outsourcing contracts (IT and non-IT). To be filled-in on a best effort basis. >	
27a	Of which, number of IT outsourcing contracts	< e.g. # of IT outsourcing contracts >	< Please provide the % with respect to total outsourcing contracts. To be filled-in on a best effort basis. >	
27b	Of which, overall number of INTRA-group IT outsourcing contracts	< e.g. # of IT intra-group outsourcing contracts >	< Please provide the % with respect to total outsourcing contracts. To be filled-in on a best effort basis. >	
28	Please select the main category of IT outsourcing type via INTRA-group outsourcing	<i.e. N/A, Application development, Web development/hosting, Application support/management, Technical support/help desk, Database development/management, Infrastructure, Cloud computing, Disaster Recovery services, Telecommunications/Network, Other>	< Please elaborate on the main category of the IT outsourcing type selected. In case "Other" option has been selected, please explain what it does refer to, the nature of the IT services outsourced, which areas does it impact. To be filled-in on a best effort basis. >	
29	Please select the main category of IT outsourcing type via EXTRA-group outsourcing	<i.e. N/A, Application development, Web development/hosting, Application support/management, Technical support/help desk, Database development/management, Infrastructure, Cloud computing, Disaster Recovery services, Telecommunications/Network, Other>	< Please elaborate on the main category of the IT outsourcing type selected. In case "Other" option has been selected, please explain what it does refer to, the nature of IT services outsourced, which areas does it impact. To be filled-in on a best effort basis. >	
30	Please indicate the main activity using CLOUD computing	<e.g. HR, market limits mgt >	< To be filled-in on a best effort basis. >	
31	How many services for critical functions are delivered by IT providers (intra and extra-group) to the entity? (as of 31.12 of reference year)	< e.g. 50 services >	< Please explain and provide a breakdown of services for critical functions delivered by IT provides (intra and extra-group) to the entity. > Please mention the 5 most services provided by IT providers of the entities in scope of the questionnaire. >	
31a	Of which, number of services for critical functions delivered by cloud providers to the entity?	< e.g. 5 critical cloud IT systems >	< Please explain and provide a breakdown of services into type of the cloud infrastructure (public/hybrid/community/private) and model (IaaS, PaaS, SaaS). > Please mention the 5 most critical services provided by cloud providers of the entities in scope of the questionnaire. >	
31b	Of which, number of services for critical functions delivered by external cloud providers to the entity	< e.g. 5 critical cloud IT systems >	< Please explain and provide a breakdown of services into type of the cloud infrastructure (public/hybrid/community/private) and model (IaaS, PaaS, SaaS). > Please mention the 5 most critical services provided by external cloud providers of the entities in scope of the questionnaire. >	
32	What was the total amount of losses (e.g. customer compensation, lost business) caused by unavailability or poor quality of outsourced services in the reference year (in EUR)?	< e.g. €10000000 >	< Please name which service providers caused the biggest amount of losses and briefly describe the root cause. >	
33	How many critical audit, on-site inspection and internal model investigation findings related to IT outsourcing risk have not been remediated for longer than 1 year? (as of 31.12 of reference year)	< e.g. 26 critical findings >	< Please mention the most critical findings not remediated for longer than 1 year, the root cause for the late remediation and an indication on when the remediation actions will be completed. Please clarify your definition of "critical". >	
	IT data integrity risk			
34	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)	< e.g. 215 end-user apps >	< Please name business units with the highest number of end-user developed application supporting activities (e.g. IT - 55; Risk Management 45; Credit Europe - 25). >	< Select Overall Risk Level >
34a	Of which, how many EUDAs support critical activities (e.g. regulatory reports such as FINREP/COREP, etc.)?	< e.g. 215 end-user apps >	< Please name business units with the highest number of end-user developed application supporting critical activities (e.g. IT - 55; Risk Management 45; Credit Europe - 25). Please clarify your definition of "critical". >	
35	How many incidents leading to significant invalid data modifications occurred in the reference year?	< e.g. 21 data integrity incidents >	< Please briefly elaborate on the most significant invalid data modification incidents Please clarify your definition of "significant". >	
36	How many cases of incorrect data submission in the supervisory reporting occurred in the reference year?	< # of incorrect data submission cases >	< Please briefly elaborate on the cases of incorrect data submission and the respective root causes. >	
36a	Of which, number of cases were due to IT issues	< # of incorrect data submission cases due to IT issues >	< Please briefly elaborate on the cases of incorrect data submision due to IT issues and the respective root causes. >	
37	How many critical audit, on-site inspection and internal model investigation findings related to IT data integrity risk have not been remediated for longer than 1 year? (as of 31.12 of reference year)	< e.g. 17 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". >	
38	What was the total amount of losses due to data-related incidents (e.g. data breaches, data integrity, data quality, timeliness of reporting) (in EUR)?	< e.g. €10000000 >	< Please mention the major loss drivers and root causes. >	

	Questions to the IT Risk Control Framework of the entities in scope Unless specified otherwise, the question shall be answered in relation to the reference year (1 January 2021 to 31 December 2021)	Answers	Maturity Level	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.		Optional column for supervised entities' internal use. Please note that the content of this column will not be considered by supervisors.
	IT governance			Strengths	Weaknesses	
	IT strategy					
1	1.1) A forward-looking, balanced IT strategy is defined, documented, periodically updated, approved by the management body and aligned with the business and risk strategies (e.g. risk tolerance).	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "IT 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "IT group strategy 2015-2017"). >	
	1.2) Senior management of the business line(s) is adequately involved in the definition of the supervised entity's strategic IT priorities and aware of the development, design and initiation of major business strategies and initiatives.	< Yes / No >				
	1.3) The IT strategy provides a holistic view of the current IT environment, the future direction, and the initiatives required to migrate to the desired future environment (incl. third party dependencies).	< Yes / No >				
	1.4) The IT strategy has an acceptable level of detail and contains measurable goals for the most important IT areas.	< Yes / No >				
	1.5) The IT 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).	< Yes / No >				
	1.6) Portfolios of IT-enabled investment programs and projects required to achieve specific strategic business objectives are actively monitored by relevant stakeholders.	< Yes / No >				
	1.7) The supervised entity analyses existing and emerging technologies.	< Yes / No >				
	IT policies, guidelines, standards and procedures					
2	2.1) The supervised entity has developed and maintained a set of policies, guidelines and procedures based on international well-recognised standards to support the IT strategy.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	
	2.2) Each policy covers at least the policy intent, goals, roles and responsibilities, coordination of departments, exception processes, scope of application, compliance approach and refers to other relevant policies, guidelines, standards and procedures.	< Yes / No >				
	2.3) Policies, guidelines, standards and procedures take into consideration industry good practices.	< Yes / No >				
	2.4) They are reviewed regularly by both the 1st and 2nd line to confirm their relevance.	< Yes / No >				
	2.5) They are enforced to all relevant staff, including external contractors.	< Yes / No >				
	2.6) The IT and security risk management framework/policies stipulate governance and oversight requirements, risk ownership and accountability and ensure the IT resilience of the supervised entity. They are approved and reviewed at least once a year by the management body.	< Yes / No >				
	IT budget					
3	3.1) The supervised entity prioritises the allocation of IT resources within all domains (i.e. for operations, projects, maintenance, security and risk management)	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	
	3.2) The IT budget reflects the priorities established by the supervised entity's IT strategy.	< Yes / No >				
	3.3) A proper cost and benefit analysis is implemented.	< Yes / No >				
	3.4) The IT budget is subject to an ongoing review, refinement and approval.	< Yes / No >				
	3.5) The IT budgeting process is transparent and accountable in order to enable the supervised entity to make informed decisions.	< Yes / No >				
	IT organisation and IT outsourcing			Strengths	Weaknesses	
	Clear roles and responsibilities and segregation of duties within IT					
4	4.1) Clear roles and responsibilities of IT personnel, including the management body and its committees are defined, which are documented and implemented in order to support the IT strategic objectives.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	
	4.2) Conflicting duties/interests and areas of responsibility are segregated to prevent unauthorized or unintentional modification or misuse of the supervised entity's assets.	< Yes / No >				
	4.3) The supervised entity engages independent IT risk control and information security functions to ensure that major risks associated with IT are identified, assessed and effectively managed in accordance with the supervised entity's approved risk tollerance.	< Yes / No >				
	4.4) IT and Information Security key roles, such as Chief Information Officer ('CIO'), Chief Operating Officer ('COO') and Chief Information Security Officer ('CISO') are well supported and have adequate access to the management body in order to escalate IT topics when needed.	< Yes / No >				
	Staffing, technical resources, qualification and training					
5	5.1) The supervised entity ensures that adequate and sufficient IT-related capabilities (human and technical resources) are available to support the IT strategy and objectives.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >	
	5.2) The supervised entity reviews staffing requirements on a regular basis or upon major changes to the business, operations or IT environments.	< Yes / No >				
	5.3) IT personnel, including external employees, have appropriate competencies to fulfil assigned roles and responsibilities based on their education, training and experience.	< Yes / No >				
	5.4) The supervised entity has defined core IT competency requirements, including competencies for IT risk management and IT security management, and verifies that they are being maintained, using qualification and certification programmes where appropriate.	< Yes / No >				
	5.5) All staff members, including key function holders, receive appropriate training on ICT and security risks, including on information security, on an annual basis, or more frequently if required.	< Yes / No >				

	Questions to the IT Risk Control Framework of the entities in scope Unless specified otherwise, the question shall be answered in relation to the reference year (1 January 2021 to 31 December 2021)	**Answers**	**Maturity Level**	**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.	
	IT outsourcing				
6	6.1) The management body and senior management are informed and make the decision whether to outsource or not, based on a documented assessment of the impact of the choice made on the risk management of the supervised entity.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). > < Please explain to what extent cloud services follow the same framework as other outsourcing services and include details about how audit rights, security, chain outsourcing, contingency plans, exit strategies, proper inventory of services and location of systems and data are considered in the context of cloud services. > <Regarding the control whether the outsourcing institution takes risk associated with chain outsourcing into account, we expected this control to follow defined process incl. identification, assessment and monitoring of any risk related to third party providers that deliver service to the institutions' outsourcing providers. Chain outsourcing risk should be considered in the overall risk assessment of an outsourced service and there should be a contractual agreement between institution and provider to be at least informed about further third party involvement by the provider or even requiring approval ex ante approval by the outsourcing institution.>	< 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). > < Please explain to what extent cloud services follow the same framework as other outsourcing services and include details about how audit rights, security, chain outsourcing, contingency plans, exit strategies, proper inventory of services and location of systems and data are considered in the context of cloud services. > <Regarding the control whether the outsourcing institution takes risk associated with chain outsourcing into account, we expected this control to follow defined process incl. identification, assessment and monitoring of any risk related to third party providers that deliver service to the institutions' outsourcing providers. Chain outsourcing risk should be considered in the overall risk assessment of an outsourced service and there should be a contractual agreement between institution and provider to be at least informed about further third party involvement by the provider or even requiring approval ex ante approval by the outsourcing institution.>
	6.2) The supervisor's right to access and to audit outsourcers is ensured contractually for all outsourcing cases (including cloud services).	< Yes / No >			
	6.3) For each outsourcing, there is a contract between the supervised entity and the service provider, defining service levels and IT security requirements, such as standards for ensuring confidentiality, availability, integrity and agility of information/IT systems, but also operational and security incident handling procedures including escalation and reporting.	< Yes / No >			
	6.4) The supervised entity defines criteria and processes to identify, assess and monitor third party service providers and concentration.	< Yes / No >			
	6.5) With regard to "chain" outsourcing, the supervised entity has contractual clauses with its outsourcers that allow at least audit rights on the "chain" outsourcer, and approval or notification if such case occurs.	< Yes / No >			
	6.6) A monitoring process is in place ensuring that the level of services procured comply with contractual agreements.	< Yes / No >			
	6.7) Individual contingency plans and exit strategies are defined and regularly updated for each outsourcing and the respective responsibilities of the provider are contractually agreed on.	< Yes / No >			
	6.8) The outsourcing policy defines roles and responsibilities, as well as competencies required to monitor and manage the risks from the IT outsourced services, including a regular risk assessment of all outsourced services.	< Yes / No >			
	6.9) The human and technical resources involved in the outsourcing processes are adequate for performing the tasks effectively and efficiently.	< Yes / No >			
	6.10) The supervised entity has an up to date register of outsourced services with at least the level of detail stated in section 11 of the EBA Guidelines on outsourcing arrangements.	< Yes / No >			
	6.11) The supervised entity's policies include procedures to inform supervisors about critical/important activities to be outsourced.	< Yes / No >			
	6.12) There is a comprehensive documented and regularly updated risk framework fully covering the outsourcing area and all outsourcing providers. The 2nd Line of Defence (LoD) and 3rd LoD have adequate expertise and resources, and they regularly and fully cover (i.e. via control mechanisms as well as Internal Audit) the outsourcing area including the providers.	< Yes / No >			
	IT risk management			**Strenghts**	**Weaknesses**
	IT risk management framework				
7	7.1) The supervised entity has an integrated and institution-wide risk culture, based on a full and common understanding of the IT risks it faces and how they are managed, taking into account its risk tolerance/appetite set by the management body ("tone from the top") and defined in the Risk Appetite Framework.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	7.2) The IT risk management framework defines: the roles and responsibilities, the internal and external context for each risk assessment, the goal of the assessment, the criteria against which the risks are evaluated, the risk management objectives, and the risk appetite and/or the risk tolerance thresholds for IT risk.	< Yes / No >			
	7.3) The IT risk management framework is approved by senior management and is regularly reviewed and, if need be, updated.	< Yes / No >			
	7.4) The roles and responsibilities, as defined in the IT risk management framework, are communicated and embedded in all relevant parts of the organisation.	< Yes / No >			
	Identification and assessment of IT risk				
8	8.1) The supervised entity maintains and regularly updates an inventory of all identified IT risks (incl. findings from internal or external audit functions).	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	8.2) All business functions and IT assets (incl. supporting processes and information assets) of the supervised entity are classified based on their criticality (i.e. availability, integrity, confidentiality).	< Yes / No >			
	8.3) The classification of IT assets is commensurate with the classification of the data processed by the IT assets.	< Yes / No >			
	8.4) Threats to IT assets are identified and assessed on a regular basis.	< Yes / No >			
	8.5) IT risks are assessed in terms of their consequences for the business (incl. financial impact, potential for business disruption, potential reputational impact, regulatory and strategic impact) and the likelihood of their occurrence on all levels (i.e. inherent risk, residual risk and reliance on control mechanisms).	< Yes / No >			
	8.6) The IT risk assessments are performed on a regular basis and on occasion of major IT changes and IT outsourcing initiatives.	< Yes / No >			
	8.7) The supervised entity has identified its risk profile in the banking sector with regard to Cybersecurity.	< Yes / No >			
	8.8) The supervised entity identifies, establishes and maintains an updated mapping of its business functions, roles and supporting processes to identify the importance of each and their interdependencies related to ICT and security risks. In addition, the supervised entity identifies, establishes and maintains an updated mapping of the information assets supporting their business functions and supporting processes, such as IT systems, staff, contractors, third parties and dependencies on other internal and external systems and processes, to be able to, at least, manage the information assets that support their critical business functions and processes.	< Yes / No >			
	IT risk management response				
9	9.1) The supervised entity has defined IT risk response strategies such as IT risk avoidance, reduction, sharing or acceptance.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	9.2) A priority order for risk response and action plans are established in an IT risk response policy. In the case of risk acceptance, formal approval processes are followed and documented, including criteria and thresholds that define level of approval to the respective risk category/level.	< Yes / No >			
	9.3) All residual risk is accepted and remains within the risk tolerance and its acceptance is formally documented.	< Yes / No >			
	Monitoring of IT risk and 2nd line of defence				
10	10.1) There is an independent IT risk control function incl. its own dedicated budget (2nd Line of Defence) with a direct reporting line to the management body.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	10.2) The effectiveness of IT risk treatment is monitored and reviewed regularly by the supervised entity.	< Yes / No >			
	10.3) Accepted residual IT risks are monitored by the IT risk control function.	< Yes / No >			
	10.4) Exceptions from IT internal rules and policies are documented and escalated to the management body.	< Yes / No >			

	Questions to the IT Risk Control Framework of the entities in scope Unless specified otherwise, the question shall be answered in relation to the reference year (1 January 2021 to 31 December 2021)	**Answers**	**Maturity Level**	**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.	
	IT security management			**Strengths**	**Weaknesses**
	Information security policies and procedures				
11	11.1) The supervised entity has established documented information security policies and procedures approved by the management body.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	11.2)These information security policies and procedures set the rules to protect the supervised entity's information assets, in line with its strategy and risk appetite and are applicable to all employees and third parties accessing information.	< Yes / No >			
	11.3) The security policies and procedures are communicated to all staff and contractors and their implementation of the security policies and procedures is supported by appropriate investments in human and technical resources.	< Yes / No >			
	Security reviews				
12	12.1) 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).	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019").
	12.2) 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.	< Yes / No >			
	12.3) Similarly, physical security (incl. appropriate redundancy levels) is regularly reviewed against best practices.	< Yes / No >			
	12.4) In order to provide objective and reliable results, security reviews are carried out by independent parties to maintain segregation of duties.	< Yes / No >			
	IT security awareness				
13	13.1) 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 IT systems and the main IT security risks (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.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	13.2) Newcomers receive mandatory training on IT security.	< Yes / No >			
	13.3) IT staff receives specific trainings on IT security.	< Yes / No >			
	13.4) The Intranet site has a dedicated section on IT security topics, guidelines and best practices.	< Yes / No >			
	Physical security				
14	14.1) The supervised entity has adequate physical security controls to protect its premises, data centres and sensitive areas (e.g. technical areas hosting cabling, UPS, backup media, etc.).	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	14.2) Physical security controls are implemented in line with the criticality of the area to be protected and the information hosted.	< Yes / No >			
	14.3) Physical security and access to premises, buildings and areas is justified, authorised, logged and monitored for employees, third parties and contractors.	< Yes / No >			
	14.4) A procedure is documented and enforced to grant, limit and revoke access to premises and building areas according to business needs, including emergency situations.	< Yes / No >			
	14.5) Furthermore, environmental controls, such as air conditioning, fire extinguishing systems, flood detectors, alternative power supply, etc., are implemented and regularly mantained to protect the supervised entity from physical hazards (fire, water damage, power cut etc.).	< Yes / No >			
	Identity and access management				
15	15.1) A documented user access management procedure approved by the management is developed, implemented, enforced, duly monitored and reviewed and in line with information risk management requirements.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	15.2) Based on the procedures, the following basic principles/processes are implemented: * Need to know and least privilege principle (only the minimum access rights strictly required to perform the job duties are assigned to the users); * Segregation of duties; * Joiners/ leavers/ move process (access rights are updated throughout the user's working life and promptly removed upon the user's departure); * Proper involvement of the information owner(s) (especially for access rights approvals); * Enforcement of sufficiently robust authentication methods including among others adequate password rules for standard, technical and privileged user accounts (e.g. password length, complexity, duration, history …); * Dedicated privileged access right management (incl. logging, monitoring, limited access, etc.); * Regular access rights reviews (recertification), especially for critical systems; * User accountability (users have nominative accounts; use of common/group accounts is very limited, justified and strictly monitored); * Protection of technical users; and * Secure treatment of temporary/external users.	< Yes / No >			
	15.3) There are specific and stronger security requirements for privileged access (e.g. jump server solution, password vault for one-time use, logging and monitoring of activities).	< Yes / No >			
	15.4) Logical access control is defined, documented, duly implemented and regularly reviewed for all IT assets.	< Yes / No >			
	Patch and vulnerability management				
16	16.1) Patch and vulnerability management is developed and implemented.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	16.2) All patching processes are triggered and performed in timely manner.	< Yes / No >			
	16.3) Vulnerabilities are identified (incl. through vulnerability scanning), centrally documented, analysed, classified and patched accordingly within an acceptable timeframe, coherent with the IT systems' criticality.	< Yes / No >			
	Network security (incl. remote access)				
17	17.1) Measures exist to protect the IT systems from attacks either from the internet extranet and intranet. These include perimeter defence technologies like firewalls, IPS/IDS, web application firewalls, web filters, mail filters, antivirus and content scanner devices (e.g. sandbox devices).	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	17.2) The supervised entity implemented appropriate procedures and security controls to protect the information while in transit through all types of communication facilities, e.g. by using encryption technologies (applied either on the line or on the information itself).	< Yes / No >			
	17.3) The supervised entity properly controls and limits (in case of critical access rights) the remote access to its system strictly to those users requiring access and with only the access rights required to perform the remote intervention or work.	< Yes / No >			
	17.4) Depending on the sensitivity of the information accessed, the remote access requires strong authentication mechanisms and it is carried out via secured communication lines.	< Yes / No >			
	17.5) Any maintenance is properly logged, including remote maintenance.	< Yes / No >			
	17.6) Internal networks are appropriately segmented.	< Yes / No >			

	Questions to the IT Risk Control Framework of the entities in scope Unless specified otherwise, the question shall be answered in relation to the reference year (1 January 2021 to 31 December 2021)	**Answers**	**Maturity Level**	**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 & monitoring				
18	18.1) The supervised entity has implemented effective measures to log and monitor security events and promptly react in case of alerts.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	18.2) 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).	< Yes / No >			
	18.3) Security events generating an alert are promptly managed/treated via a coordinated security incident management process.	< Yes / No >			
	18.4) 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.	< Yes / No >			
	18.5) 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.	< Yes / No >			
	18.6) The Senior Management is timely informed about the IT security incidents detected in the organisation including their consequences, organisation reaction and additional controls implemented..	< Yes / No >			
	Malware prevention				
19	19.1) The supervised entity has implemented adequate protection against malware (e.g. antivirus, advanced malware prevention solutions, sandboxes).	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	19.2) 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). Malware prevention on mobile devices can be achieved by equivalent lockdown and monitoring measures in accordance with the current industry best practice.	< Yes / No >			
	19.3) The malware prevention software is updated regularly and technical measures prevent end users from deactivating this.	< Yes / No >			
	Data classification				
20	20.1) 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).	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	20.2) In order to properly conduct the data classification, clear owners of the information (categories) are determined	< Yes / No >			
	20.3) Data classification policies and procedures describe what measures are applied based on the classified criticality/sensitivity of the information.	< Yes / No >			
	20.4) Protection against data leaks is implemented, properly managed and continuously monitored.	< Yes / No >			
	IT operations management			**Strengths**	**Weaknesses**
	Asset inventory and configuration management				
21	21.1) The supervised entity maintains an up-to-date inventory of all IT assets/ configuration items (software and hardware including outsourced assets) with at least the following level of detail: title, description, state, actual configuration, ownership and criticality of all IT assets/ configuration items as well as their relationship among each other (e.g. upstream and downstream dependencies).	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	21.2) The inventory identifies the critical assets and the corresponding recovery requirements, and the interdependencies/ data flows between different assets.	< Yes / No >			
	21.3) Configuration baselines are established by defining a set of standard configuration setups and hardening rules.	< Yes / No >			
	Backups				
22	22.1) The supervised entity backs up its IT 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.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	22.2) 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 IT systems.	< Yes / No >			
	22.3) The management of the offsite storage facility complies with the data classification policy and the supervised entity's media storage practices.	< Yes / No >			
	22.4) Depending on the sensitivity of the information involved, backups are encrypted to protect the information in case of loss or voluntary/accidental alteration.	< Yes / No >			
	22.5) Backups are regularly tested to ensure they are not corrupted.	< Yes / No >			
	IT operations (incl. job scheduling, system monitoring, capacity management…)				
23	23.1) The supervised entity has documented and implemented procedures to ensure the standard operations of its IT systems. Such procedures include (but not limited to): job scheduling processes; logging and monitoring of IT 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.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	23.2) 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 IT assets are regularly reviewed, maintained and repaired as befitting their criticality.	< Yes / No >			
	23.3) 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.	< Yes / No >			
	Incident and problem management				
24	24.1) 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).	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	24.2) Incidents and service requests are identified, logged (by way of dedicated service desk tools), categorized and prioritised according to business criticality and service agreements.	< Yes / No >			
	24.3) Notifications from detection systems are investigated in a timely manner and when required, response plans are swiftly executed and forensics are performed.	< Yes / No >			
	24.4) 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.	< Yes / No >			
	24.5) If required, escalation might involve notification to relevant authorities.	< Yes / No >			
	24.6) 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 process, 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.	< Yes / No >			

	Questions to the IT Risk Control Framework of the entities in scope Unless specified otherwise, the question shall be answered in relation to the reference year (1 January 2021 to 31 December 2021)	Answers	Maturity Level	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.	
	Change and release management				
25	25.1) A formal and documented process is in place for managing and controlling changes to IT systems.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	25.2) Changes are defined, prioritised, formally approved, planned, tested and transitioned in a consistent and coordinated way.	< Yes / No >			
	25.3) Significant changes are scheduled for implementation and approved by a dedicated management committee.	< Yes / No >			
	25.4) 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.	< Yes / No >			
	25.5) Development and test environments do not contain confidential production data and test environments adequately reflect the production environment.	< Yes / No >			
	25.6) The deployment of changes into production environment is only conducted by authorised production teams after a formal change approval.	< Yes / No >			
	25.7) Changes to IT security controls (e.g. to firewall rules) are authorised by relevant Information/IT security managers (e.g. CISO) after having analysed the IT security impacts.	< Yes / No >			
	25.8) 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.	< Yes / No >			
	25.9) A release management team that directs the IT departments' decisions about production setting, ensuring a holistic view of changes to IT systems, is in place.	< Yes / No >			
	IT project management			**Strengths**	**Weaknesses**
	Project management framework and governance				
26	26.1) A project management framework is in place for the management of all IT 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.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	26.2) Project governance and oversight processes are implemented to effectively support the management and monitoring of IT projects (e.g. project management office, an IT steering committee or equivalent) and include appropriate reporting of the establishment and progress of IT projects and their associated risks to the management body at an adequate frequency.	< Yes / No >			
	26.3) Project oversight for the development of any critical system is assigned to the IT steering committee.	< Yes / No >			
	26.4) The projects of the supervised entity are consistent with its strategy.	< Yes / No >			
	26.5) The projects are initiated with an approved scope, benefits, objectives and identified key stakeholders.	< Yes / No >			
	26.6) Dependencies between projects are identified, analysed, evaluated and managed by an overarching function.	< Yes / No >			
	26.7) A project independent quality assurance is implemented.	< Yes / No >			
	IT solutions life cycle				
27	27.1) IT 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).	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	27.2) Information security (including cyber security) requirements are included in the requirements defined for new information systems or enhancements to existing information systems.	< Yes / No >			
	27.3) IT security controls are implemented for all phases of the IT solutions life cycle, starting from the design, development (incl. measures to protect the integrity of the source codes of IT systems that are developed in-house), purchasing and testing phases and continuing through the operation phase.	< Yes / No >			
	27.4) The IT solutions life cycle standards, methodologies and safeguards also apply to End User Computing (EUC).	< Yes / No >			
	Data quality management			**Strengths**	**Weaknesses**
	Data quality management				
28	28.1) Data quality management procedures are defined, documented and tested.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	28.2) Roles and responsibilities regarding data quality are clearly defined.	< Yes / No >			
	28.3) A Chief Data Office(r), or an equivalent function, is formally established.	< Yes / No >			
	28.4) The supervised entity's human and technical resources are sufficient to support an adequate level of data quality.	< Yes / No >			
	28.5) Data quality management procedures include proper IT controls (e.g. automated input validation controls, data transfer controls, reconciliation, etc.) for the different phases of the IT 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.	< Yes / No >			
	28.6) 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.	< Yes / No >			
	28.7) Data quality management procedures also apply to End User Computing (EUC).	< Yes / No >			
	Data architecture model				
29	29.1) The supervised entity has defined and documented its data architecture, data models and data flows, and validated them with relevant business and IT stakeholders.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	29.2) The data architecture is regularly reviewed (and updated if needed)	< Yes / No >			
	29.3) Golden (authoritative) sources are defined for business critical applications.	< Yes / No >			
	29.4) Data dictionaries are maintained for critical business applications.	< Yes / No >			

	Questions to the IT Risk Control Framework of the entities in scope Unless specified otherwise, the question shall be answered in relation to the reference year (1 January 2021 to 31 December 2021)	Answers	Maturity Level	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.	
	IT continuity management			**Strengths**	**Weaknesses**
	IT continuity and disaster recovery - risk analysis, assessment and treatment				
30	30.1) The supervised entity has formally documented processes for analysing, approving and treating IT continuity risks in place.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	30.2) It keeps an inventory of its critical activities, services and resources which is updated regularly and securely stored.	< Yes / No >			
	30.3) Critical operations and interconnections (i.e. end to end mapping) are mapped.	< Yes / No >			
	30.4) Possible impacts of disruptions in services with regards to the business processes are assessed (e.g. by conducting a business impact analysis). As a result, appropriate recovery time objectives, recovery point objectives, and maximum tolerable downtimes are defined.	< Yes / No >			
	30.5) When procuring solutions or services that are (or will become) important for the continuity of critical activities / services, the supervised entity checks during the selection process whether continuity requirements are met.	< Yes / No >			
	IT continuity and disaster recovery - plans, processes and procedures				
31	31.1) The supervised entity has an appropriately documented crisis management framework in place and regularly reviews plans, processes and procedures to enable the continuity and recovery of critical IT systems and services (including outsourced systems and services) from a range of realistic scenarios (e.g. loss of staff, loss of building(s), loss of external service provider(s), loss of IT system(s), cyber-attacks, etc.) as well as effective crisis communication in such a scenario.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	31.2) Continuity and recovery plans are designed, maintained, regularly updated and approved by the management body offering short-term, alternative (where recovery may not be feasible in the short term because of costs, risks, logistics or unforeseen circumstances) and long-term recovery options to minimize disruption to the supervised entity's operations within acceptable limits.	< Yes / No >			
	31.3) Continuity and recovery plans are also updated on an ad-hoc basis where required (e.g. in case of structural changes of the IT systems or a based on lessons learned from major incidents - whether bank-internal incidents or external incidents).	< Yes / No >			
	IT continuity and disaster recovery - technical infrastructure and solutions				
32	32.1) For the critical activities and services, the supervised entity makes use of redundant and secure technical infrastructure (e.g. data centres (local and regional) , load balancers monitoring/capacity solutions, denial of service solutions, etc.).	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	32.2) Procedures and solutions for redundant and secure data storage and back-up are in place.	< Yes / No >			
	IT continuity and disaster recovery - testing & continuous improvement				
33	33.1) BCPs/response and recovery plans are tested periodically. BCPs/response and recovery plans of critical business functions, supporting processes, information assets and their interdependencies (including those provided by third parties, where applicable) are tested at least annually.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	33.2) All relevant stakeholders participate in the tests and the management body and senior management are appropriately involved and informed.	< Yes / No >			
	33.3) Test results are formally documented and used to strengthen the effectiveness of the crisis management procedures and protective measures.	< Yes / No >			
	33.4) Furthermore, the results of the contingency tests are communicated to the responsible members of staff.	< Yes / No >			
	33.5) For time-critical activities and processes that are outsourced, the supervised entity and the external service provider have contingency plans that are coordinated with each other.	< Yes / No >			
	IT reporting			**Strengths**	**Weaknesses**
	IT reporting				
34	34.1) An IT reporting process is designed with clear structural and operational rules, defining responsibilities, subjects of reports, deadlines, communication channels, etc. and ensuring that the IT reporting is performed with the appropriate level of accuracy, integrity, completeness, comprehensiveness, clarity, usefulness and timeliness.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	34.2) Secured channels are used for the distribution of IT reports.	< Yes / No >			
	34.3) The IT reporting system includes the reporting of the IT service provider (e.g. cloud service provider), in case of an outsourced activity.	< Yes / No >			
	34.4) IT reporting is performed on a regular basis, providing information to relevant recipients (e.g. senior management) to identify, assess, monitor and manage the supervised's IT risk considering the approved risk appetite.	< Yes / No >			
	Internal IT audit			**Strengths**	**Weaknesses**
	Internal IT audit				
35	35.1) The IT risk control framework is audited with the required quality, depth and frequency and commensurate with the size, activities and the IT risk profile of the supervised entity. A comprehensive and detailed IT audit universe is established.	< Yes / No >	< Select Overall 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) 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 ("N" has been chosen as answer), 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 ("Y") has been chosen as answer) the title(s) of the most relevant evidence should be mentioned here (for example "Guideline x; Procedure A; Report B 2019"). >
	35.2) The audit plan includes critical IT risks identified by the supervised entity (including those of outsourced activites) and takes into consideration the results of previous audits.	< Yes / No >			
	35.3) IT audit findings, including agreed actions, are followed up and progress reports are periodically reviewed by the senior management and/or the audit committee.	< Yes / No >			
	35.4) There is procedure for ad hoc reporting to the management body based on the criticality of the findings reported by IT audits.	< Yes / No >			
	35.5) The internal audit function has adequate resources, both in terms of number of staff and of competences/skills, to properly perform IT Audit activities.	< Yes / No >			

IT Risk Level Guidance

Risk Level →	1 (Lowest exposure)	2	3	4 (Highest exposure)	COMMENT	RISK DEFINITION (EBA-GL-2017-05)
Risk Category ↓	*IT risk levels should be assessed by taking into account their* ***inherent risks*** *and potential losses if these risks were to materialise.*					
IT 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 IT 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 IT 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 IT systems.	The supervised entity would suffer high impact in case of unauthorized access because of sensitive data on its IT 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).
IT availability and continuity risk	The supervised entity would suffer no impact if IT 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 IT 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 IT systems were to be unavailable for an extended period.	The supervised entity would suffer high impact if IT 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.
IT change risk	There is a low frequency of significant changes to critical IT 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 IT systems and limited bug fixes were required to fix unplanned outages caused by changes.	There is a medium frequency of significant changes to critical IT systems.	There is a high frequency of significant changes to critical IT 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.
IT outsourcing risk	There are no outsourced service providers (including intra-group) used by the supervised entity (i.e. no losses due to poor quality of outsourced services, no critical findings).	There are a small number of non-key services outsourced to service providers, including intra-group. Additionally, only minor losses were caused by poor quality of key outsourced services.	There are some key services outsourced to service providers (including intra-group).	There are a large proportion of key services outsourced to service providers (including intra-group).	*Intra-group means a different legal entity than the supervised entity, but within the same group*	The risk that engaging a third party, or another Group entity (intra-group outsourcing), to provide ICT systems or related services adversely impacts the supervised entity's performance and risk management.
IT data integrity risk	Golden sources of data are defined to cover all core business activities, and all manual or automated transfers/inputs have layers of controls to check consistency. 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. Several databases are fed with the same 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.

IT Risk Control Guidance

Criteria to consider →	A	B	C	D	E	F	G	H	I	J	Summary (see below for more detail on criteria)
Risk Control Level ↓	IT risk controls should be assessed by how effectively they mitigate IT risks.										
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 currently underway to address any issues.

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.	
Cloud computing	Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e. g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.	EBA/CP/2017/06
Collateral optimisation services	Services that are offered to match collateral supply and collateral demand for a given market participant and seek to enhance the efficiency of collateral use for the market participant based on algorithms and other tools employed by the service provider. Optimisation services may include a transaction component, whereby the service provider is authorised to automatically transfer, reposition or post collateral on behalf of the market participant. The use of collateral can be optimised in different ways. Multi-factor algorithms consider transaction costs, tax implications; cash balance thresholds, expected future demand, concentration issues and eligibility constraints of potential future counterparties. This allows to apply dynamic optimisation through algorithms such as “best to recall” (collateral in excess is recalled) and “best to substitute” (existing collateral is substituted with other eligible assets when this is deemed preferable).	ECB memo of 12 September 2016 on "Technological innovation in the financial sector"
Critical IT System	Critical ICT systems and services fulfil at least one of the following conditions: a. they support the core business operations and distribution channels (e.g. ATMs, internet and mobile banking) of the institution; b. they support essential governance processes and corporate functions, including risk management (e.g. risk management and treasury management systems); c. they fall under special legal or regulatory requirements (if any) that impose heightened availability, resilience, confidentiality or security requirements (e.g. data protection legislation or possible ‘Recovery Time Objectives’ (RTO, the maximum time within which a system or process must be restored after an incident) and ‘Recovery Point Objective’ (RPO, the maximum time period during which data can be lost in case of an incident)) for some systemically important services (if and where applicable)); d. they process or store confidential or sensitive data to which unauthorised access could significantly impact the institution’s reputation, financial results or the soundness and continuity of its business (e.g. databases with sensitive customer data); and/or e. they provide base line functionalities that are vital for the adequate functioning of the institution (e.g. telecom and connectivity services, ICT and cyber security services).	EBA/GL/2017/05
Critical or Important Function	In the context of outsourcing, according to section 4 of the EBA GLs on Outsourcing Arrangements, functions of which a defect or failure in a its performance would materially impair (i) continuing compliance with the conditions of the institution's authorisation, (ii) their financial performance or (iii) the soundness or continuity of their banking and payment systems. In addition, outsourcing of operational tasks of internal control functions (unless a failure would not lead to an adverse impact on the effectiveness of internal controls) or the outsourcing of banking activities/payment services that require authorisation.	EBA/GL/2019/02, para. 29 following
Crowdfunding	Crowdfunding is the practice of funding a project or venture by raising monetary contributions from a large number of people, today typically performed via internet-based systems.	ECB memo of 12 September 2016 on "Technological innovation in the financial sector"
Cyber attack	An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.	NIST, ISACA
Disaster Recovery Plan (DRP)	Documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster	
Distributed ledger technologies	Technologies that are understood to be included block chains, consensus ledgers and smart contracts, used in trading, post-trading (i.e. clearing and settlement), and/or cross-border payment arrangements. A distributed ledger is an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within the network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes or seconds. The security and accuracy of the assets stored in the ledger are maintained cryptographically through the use of ‘keys’ and signatures to control who can do what within the shared ledger. Entries to the ledger can be updated by one, some or all of the participants, according to rules agreed by the network. Due to the fact that distributed ledgers no longer require a central authority and their application beyond payments from where DLTs started (bitcoin and other virtual currencies), they might have a larger disruptive potential than other innovations.	ECB memo of 12 September 2016 on "Technological innovation in the financial sector"
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
End-of-life	A term used with respect to a product supplied to customers, indicating that the product is in the end of its useful life, and the vendor stops marketing, selling, or rework sustaining it. The vendor may simply intend to limit or end support for the product.	
Extra group outsourcing	An extra-group outsourcing is an arrangement in which the service provider does not belong to the same corporate group as the outsourcing entity that is supervised by the SSM.	
Financials	The Financials section of the General Data sheet should be closely aligned to the FINREP reporting of the SIs. For the 2022 exercise (reference date Dec-21), this would be on an best effort basis with additional cross validation checks to be introduced for exercises afterwards to achieve an alignment as close as possible. 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 IT applications where exposures and positions are managed, but more often the accounting system is recognised as a golden source	BCBS 239
IAM (Identity Access Management)	Identity and access management (IAM) is a framework for business processes that facilitates the management of electronic or digital identities. The framework includes the organizational policies for managing digital identity as well as the technologies needed to support identity management	
Instant payments	Instant payments are resulting in immediate or close-to-immediate interbank clearing of transactions and crediting of the payee’s account. Instant payments require instant clearing.	ECB memo of 12 September 2016 on "Technological innovation in the financial sector"
Intra group outsourcing	An intra-group outsourcing is an arrangement in which the service provider belongs to the same corporate group as the outsourcing entity that is supervised by the SSM. In case the service provider sub-outsources the entire service to a provider outside of the corporate group, the initial outsourcing should not be considered an intra-group outsourcing.	
IT availability and continuity risks	The risk that performance and availability of IT systems and data are adversely impacted, including the inability to timely recover the institution’s services, due to a failure of IT hardware or software components; weaknesses in IT system management; or any other event.	EBA/GL/2017/05
IT budget	Estimated costs for the functioning and the development of the IT, covering both ‘run’ IT, meaning the ongoing costs of operating and maintaining the current IT systems and services, and ‘change’ meaning the development and the implementation of new IT systems (business application and IT infrastructure) and services , including the enterprise’s portfolio of IT-enabled investment programmes An IT budget should be segmented to include the following: support /maintenance of the IT environment, network and infrastructure, hardware, software, cloud services, backup, disaster recovery and business continuity, projects, miscellaneous/IT emergencies.	
IT change risk	The risk arising from the inability of the institution to manage IT system changes in a timely and controlled manner, in particular for large and complex change programmes.	EBA/GL/2017/05
IT data integrity risk	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 institution to provide services and produce (risk) management and financial information in a correct and timely manner.	EBA/GL/2017/05

Term	Definition	Source
IT governance	The processes that control for adequate internal governance and internal control framework being in place for the management of ICT and security risks, including adequate management of ICT systems, roles and responsibilities, risk management frameworks, budget allocation, staff training, and implementation of the ICT strategy.	Based on EBA/GL/2019/04
IT internal audit	An independent and risk-based approach review of ICT and security-related activities and units to ensure compliance with the institution's policies and procedures and with external requirements.	Based on EBA/GL/2019/04
IT outsourcing risk	The risk that engaging a third party, or another Group entity (intra-group outsourcing), to provide ICT systems or related services adversely impacts the institution’s performance and risk management.	EBA/GL/2017/05
IT resilience	IT (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
IT risk	The risk of loss, material or potential, due to breach of confidentiality, failure of integrity of systems and data, unavailability of systems and data, and inability to change IT within reasonable time and costs when the environment or business requirements change (i.e. agility)”	EBA/GL/2017/05
IT security risk	The risk of unauthorised access to IT systems and data from within or outside the institution (e.g. cyber-attacks).	EBA/GL/2017/05
IT services	Services provided by IT systems to one or more internal or external users. Examples include data entry, data storage, data processing and reporting services, but also monitoring, business and decision support services. An IT Service is based on the use of Information Technology and supports the customer’s business processes. It is made up from a combination of people, processes and technology and should be defined in a Service Level Agreement.	EBA/GL/2017/05; COBIT & ITIL
IT system	IT set-up as part of a mechanism or an interconnecting network that support the operations of an institution.	EBA/GL/2017/05
Malware (malicious software)	Any program or file that is harmful to a computer user, which includes computer viruses, worms, Trojan horses and spyware.	
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
Outsourcing Register	An updated register of information on all outsourcing arrangements at the institution, which should appropriately document all current outsourcing arrangements, distinguishing between the outsourcing of critical or important functions and other outsourcing arrangements.	EBA/GL/2019/02, para. 52
Peer-to-peer (P2P)	Peer-to-peer lending is the practice of lending money to individuals or businesses through online services that match lenders directly with borrowers.	ECB memo of 12 September 2016 on "Technological innovation in the financial sector"
Robo advice	Financial advice providing portfolio management services online with minimal human intervention through automated investment solutions based on algorithms. Robo-advice presents investors with an interesting value proposition, including price reductions as much as 70 percent for some services	ECB memo of 12 September 2016 on "Technological innovation in the financial sector"
RPO (recovery point objective)	Point to which data must be restored to enable the activity to operate on resumption.	ISO 22301:2012
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 centralised unit that deals with security issues on an organizational and technical level. A SOC is equipped for monitoring IT security and managing IT security incident.	
SSM Countries	All euro area countries participate automatically in the SSM. As of 2021: Austria, Belgium, Cyprus, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Portugal, Slovakia, Slovenia, Spain. A list of all EU member using the euro is available at https://www.ecb.europa.eu/euro/intro/html/map.en.html	Euro area
Supervised Entity	Outline of the ECB investigatory powers.	Article 10(1) of the SSM Regulation
Supervisory Reporting	Supervisory reporting includes all the regular submission to the supervisor: COREP, FINREP, STE and STE-equivalent (as NPL reporting).	