SAQ - Art. 29-1 & 29-2 of the LFS - Low, Medium, and High Risk

Risk Levels

Section	Risk subcategory	Number	Questions	Answers	Overall Risk Level Self-assessment	Explanation Please indicate here strengths and weaknesses leading to the self-assessment score
Operational	**Operational risk**	1	How many times were the operations not run in a timely manner during the reference year?	< e.g., 5 times >	< Select Overall Risk Level >	< Please include reference to the date and short description of the reasons >
Operational		2	How many times did the client miss a regulatory deadline because of delays for which the support PFS was responsible, during the reference year?	< e.g., 5 times >		< Please mention the most significant customer service disruptions and the main root causes for these delays (in hours) and short description of the reasons including the reasons of the delay, processes impacted, and missed deadlines. >
Operational		3	How many significant operational incidents (e.g., ICT incidents, loss, alteration or misallocation of information, processing errors, etc.), affecting client data accuracy and integrity, occurred in the reference year?	< e.g., 21 data integrity incidents >		< Please briefly elaborate on the most significant operational incidents affecting client data accuracy and integrity, specifying also wrongly submitted data in supervisory reporting. Please clarify your definition of "significant". >
Operational	**IT security risk**	4	How many external staffs (including freelance consultants and/or cascade subcontractors) have any kind of access to sensitive or critical data, confidential data (including client data), and for a period longer than 1 month ?	< e.g., 30 staffs >	< Select Overall Risk Level >	< Please specify which external companies typically have the most frequent access to your sensitive or critical data, confidential data (including client data) and why. Please specify the number of external staffs (freelance and/or individuals belonging to external companies) that have any kind of access to sensitive or critical data, confidential data (including client data) >
Operational	**Outsourcing risk**	5	How relevant are outsourced services (intra- and extra-group) for critical activities in client operations?	< i.e., 1. Fully outsourced, 2. Largely outsourced, 3. Partially outsourced, 4. All in-house >	< Select Overall Risk Level >	< Please specify which critical activities in client operations have been outsourced to which major IT service providers. Name major service providers and specify if they belong to the group or not. >
Operational		6	What is the overall number of outsourcing providers both INTRA-group and EXTRA-group?	< e.g., # of outsourcing providers >		< Please briefly describe main types of outsourcing providers. >
Transversal	**Operational risk**	1	Number of IT employees in FTE (all IT functions including IT security and IT risk management; internal staff and external staff that has been working for longer than 6 months in the institution).	< # of Internal FTEs >	< Select Overall Risk Level >	< Please describe where the largest number of IT staff is employed for the entities in scope, how many positions are vacant and how many positions are planned to be created/abolished for the year after the reference year. This shall include external staff that have been working for longer than 6 months in the institution. Resources working remotely are resources operating outside Luxembourg and dedicated to the service provision to the Support PFS >
Transversal				< # of External FTEs working in Luxembourg >		
Transversal				< # of Group FTEs working in Luxembourg >		
Transversal				< # of External FTEs working remotely >		
Transversal				< # of Group FTEs working remotely >		
Transversal		2	Staff turnover rate in IT departments of the entities in scope for the reference year (IT staff leaving the entities in scope; including IT security and IT risk management)?	< % of IT staff (both External and Internal) turnover (including IT risk and IT/information security) >		< Please briefly elaborate on areas with the highest staff turnover rate. Please explain how the staff turnover rate for IT departments is seen compared to the overall staff turnover for the entities in scope.>
Transversal				< % of total staff turnover >		

Section	Risk subcategory	Number	Questions	Answers	Overall Risk Level Self-assessment	Explanation Please indicate here strengths and weaknesses leading to the self-assessment score
Transversal	**IT security risk**	3	Number of locations of significant IT functions, data centres and business functions in scope	< # of IT function and data centre locations >	< Select Overall Risk Level >	< 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., Luxembourg - 2; Kayl - 4; Windhof - 4; etc. >
Transversal				< # of business locations >		
Transversal		4	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 main types 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.). >
Transversal				< average time for detection (all type of cyber-attacks - in hours) >		< Please briefly explain the main types 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.). >
Transversal				<average time for recovery (all type of cyber-attacks - in hours) >		
Transversal				<average time for detection (cyber-attacks excluding DDOS - in hours) >		
Transversal				<average time for recovery (cyber-attacks excluding DDOS - in hours)>		
Transversal		5	How often is Information Security part of the agenda of the Authorised Management?	< select Frequency category >		< e.g., Formally discussed IS matters should be officially recorded in the minutes of the board meeting >
AML/CFT	**Money laundering and terrorist financing risk**	1	How many financial sector clients are classified as low-risk from an ML/TF perspective?	< enter the number of financial sector's clients you classified as low-risk in your data base for the year under review>	< Select Overall Risk Level >	If you have more than 3 categories, please regroup them into the 3 proposed categories for the purpose of this reporting.
AML/CFT		2	How many financial sector clients are classified as medium-risk from an ML/TF perspective?	< enter the number of financial sector's clients you classified as low-risk in your data base for the year under review>		If you have more than 3 categories, please regroup them into the 3 proposed categories for the purpose of this reporting.
AML/CFT		3	How many financial sector clients are classified as high-risk from an ML/TF perspective?	< enter the number of financial sector's clients you classified as low-risk in your data base for the year under review>		If you have more than 3 categories, please regroup them into the 3 proposed categories for the purpose of this reporting.
AML/CFT		4	On what frequency the Support PFS performs name screening of all its financial sector clients, their beneficial owners and their representatives against international financial sanction lists (i.e., UE, UN and Luxembourg lists)?	< e.g., daily >		< Please list sources used for international financial sanction lists >
AML/CFT		5	On what frequency the Support PFS performs name screening of its financial sector clients, their beneficial owners and their representatives against PEP lists?	< e.g., every 6 months >		< Please list sources used for PEP lists >
AML/CFT		6	How many suspicious activity/transaction reports did the Support PFS submit to the Financial Intelligence Unit (Cellule de Renseignement Financier) during the year under review?	< number >		< Please briefly explain the main types of suspicious activities/transactions reported >

Risk Controls

						Explanations Please indicate here strengths and weaknesses leading to the self-assessment score	
Section	**Topic**	**Number**	**Questions**	**Answers**	**Maturity Level**	**Strengths**	**Weaknesses**
Operational	**IT security management**	**Number**	**Questions**	**Answers**	**Maturity Level**	**Strengths**	**Weaknesses**
Operational	**Data Confidentiality**	OPS-01	Access controls are enforced to restrict access solely to authorized personnel, safeguarding sensitive data, systems, and applications. Such controls are applied both to internal and external personnel. Accesses are granted on a need-to-know basis (Role-Based Access Control) and in line with the principle of segregation of duties.	< 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"). >
Operational		OPS-02	Logical accesses are reviewed at least on an annual basis to ensure that they remain granted in line with the need-to-know and principle of segregation of duties.	< Yes / No >			
Operational	**Client activities**	**Number**	**Questions**	**Answers**	**Maturity Level**	**Strengths**	**Weaknesses**
Operational	**Data Accuracy and Integrity**	OPS-03	For procedures related to client activities requiring a support PFS license, relevant data validation checks and quality assurance processes (e.g., 4 eyes principles) are put in place to: - ensure the accuracy and reliability of client information processed, - avoid loss of information (e.g., the information was wrongly indexed and can't be found anymore in the system) or misallocation of information (e.g., the information is communicated/allocated to a wrong client, or the contact details of the recipient are not up-to-date). - avoid accidental deletion or alteration of information (while the retention period requires the information to be kept). - avoid information that is supposedly destructed but still readable, or not destructed according to operational procedures, or lost before being destructed. In the case of cascade outsourcing, monitoring and oversight of the outsourced activities or services enable the achievement of identical 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 "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"). >

Operational	Client activities	Number	Questions	Answers	Maturity Level	Strengths	Weaknesses
Operational	**Environmental controls**	OPS-04	Operational efficiency (including timely processing) is achieved through the establishment of pre-agreed standardized processes with clients, incorporating customized checklists with legal deadlines, utilizing workflow management tools, optimizing resource allocation, and conducting thorough setup and testing prior to going live. In the case of cascade outsourcing, monitoring and oversight of outsourced activities further guarantee the realization of these 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 "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"). >
Operational	**Operational Efficiency**	OPS-05	For support PFS offering archiving services only: To address the risk of an inefficient archiving system (e.g., difficulties in finding an indexed document, unacceptable waiting time when retrieving an archived document, etc.), the support PFS has implemented a set of measures such as: - advanced indexing and categorization, - modern document management software with search and version control capabilities, - user training and support, - regular system maintenance, - automation of processes with OCR technology, - intuitive user interface, - evaluation of the scalability, - robust data security measures, - iterative improvement process based on user feedback.	< 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"). >

Transversal	IT continuity management	Number	Questions	Answers	Maturity Level	Strengths	Weaknesses
Transversal	**Environmental controls**	CROSS-01	The support PFS has to prevent or reduce the consequences of events originating from physical and environmental threats (natural disasters and other intentional or unintentional physical threats to infrastructure, including fire, flood, earthquake, 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 "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"). >

Transversal	IT security management	Number	Questions	Answers	Maturity Level	Strengths	Weaknesses
Transversal	**Data Confidentiality**	CROSS-02	Physical accesses are granted based on the need to know and least privilege principles, in order to restrict accesses to sensitive locations such as IT rooms, client archives storage areas, or strategic rooms (which could contain sensitive or critical data, confidential data, and/or technical areas hosting cabling, UPS, backup media, etc.). Physical security controls and measures are implemented to support that objective.	< 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"). >
Transversal		CROSS-03	Physical accesses are reviewed at least on an annual basis to ensure that they remain granted in line with the need-to-know.	< Yes / No >			

Transversal	Client activities	Number	Questions	Answers	Maturity Level	Strengths	Weaknesses
Transversal	**Client services reporting**	CROSS-04	The support PFS provides its clients with reporting on its services. The information provided as part of this reporting helps the clients to monitor and manage the performance of these outsourced services effectively, in accordance with the requirements of circular CSSF 22/806 as well as contractually agreed reporting measures. For example, a reporting package is sent on a regular basis (e.g., monthly/quarterly) to the relevant client representative including KPIs.	< 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"). >
Transversal	**Contractual provisions**	CROSS-05	The template of the contracts signed with clients of the financial sector is in line with the requirements of the CSSF circular 22/806 and includes the key contractual provisions set out in the CSSF circular 22/806.	< 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"). >

Transversal	Client activities	Number	Questions	Answers	Maturity Level	Strengths	Weaknesses
Transversal	**Client emergency communication procedure**	CROSS-06	An emergency communication procedure is defined to inform without delay clients in case of incidents or adverse events which impact or are likely to impact the service delivery or client data.	< 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"). >

Transversal	Risk management	Number	Questions	Answers	Maturity Level	Strengths	Weaknesses
Transversal	**Identification and assessment of risk (incl. ICT Risk)**	CROSS-07	The supervised entity maintains and regularly updates a register of all identified risks (self-assessment, as well as 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 "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"). >
Transversal		CROSS-08	The risk assessments are performed on a regular basis and on occasion of major changes, outsourcing initiatives or incidents.	< Yes / No >			
Transversal	**Risk management response (incl. ICT Risk)**	CROSS-09	The supervised entity has defined risk response strategies such as 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 "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"). >
Transversal		CROSS-10	A priorities order for risk response and action plans are established in a 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 >			

Transversal	Risk management	Number	Questions	Answers	Maturity Level	Strengths	Weaknesses
Transversal	**Risk monitoring and 2nd line of defence (incl. ICT Risk)**	CROSS-11	There is an independent risk control function (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 "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"). >

AML/CFT	Money laundering and terrorist financing risk	Number	Questions	Answers	Maturity Level	Strengths	Weaknesses
AML/CFT	**Money laundering and terrorist financing risk**	AML-01	The Support PFS has implemented, and periodically reviews, policies and procedures regarding AML/CFT and international financial sanctions, to ensure that they are compliant with applicable Luxembourg AML/CFT and international financial sanctions' laws, regulations and CSSF circulars. The policies have to be approved by the board of directors and the procedures by the authorised management. Both have to be communicated to the staff.	< 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"). >
AML/CFT		AML-02	The support PFS has assessed the ML/TF risks of all its financial sector clients according to risk categories (e.g., low, medium and high).	< Yes / No >			
AML/CFT		AML-03	The support PFS obtains for all its financial sector clients relevant KYC documentation in accordance with the ML/TF risk level classification and performs periodic reviews of the client's files and keeps information up-to-date.	< Yes / No >			
AML/CFT		AML-04	The suppport PFS has decided to apply simplified due diligence measures to lower risk clients.	< Yes / No >			
AML/CFT		AML-05	The support PFS has an automated *name screening* system or performs the screening manually.	< Yes / No >			
AML/CFT		AML-06	The support PFS is registered on the goAML web platform to file suspicious activity/transaction with the Financial Intelligence Unit (Cellule de Renseignement Financier)	< Yes / No >			

Risk Level Guidance

Risk Level →	1 (Lowest exposure)	2	3	4 (Highest exposure)	COMMENT	RISK DEFINITION (EBA-GL-2017-05)
Risk Category ↓	*Risk levels should be assessed by considering their **inherent risks** and potential losses if these risks were to materialise.*					
IT security risk	The support PFS would suffer no/negligible impact in the event of unauthorized access because it does not hold sensitive data on its IT systems (i.e., no incidents, no data breaches, no critical findings).	The support PFS would suffer limited impact in case of unauthorized access because it holds limited sensitive data on its IT systems (i.e., very low number of incidents, negligible losses due to data breaches).	The support PFS would suffer medium impact in case of unauthorized access because of sensitive data on its IT systems.	The support PFS 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 institution (e.g., cyber-attacks).
Operational risk	Isolated incident(s) with manageable impact(s) on clients	Isolated incident(s) with significant impact(s) on clients / interruption of an entire process	Systemic incident(s) with impact(s) on several clients / partial stop of activities	Complete stop of activities		
Legal risk	Deficiency letter / request by CSSF to state its position Commercial dispute(s) / creation of provisions	Regular breach - threat to fine / injunction by CSSF / Civil case / dispute with isolated client	Serious breach - fine / dismissal of management / threat by CSSF to withdraw authorisation / Criminal case / dispute with mass clients	Loss / withdrawal of authorisation by CSSF / Payment suspension / liquidation of the company		
IT availability and continuity risk	The support PFS would suffer no impact if IT systems were to be unavailable for an extended period (i.e., no loss due to unplanned downtime of critical systems, no critical findings).	The support PFS would suffer limited impact if IT systems were to be unavailable for an extended period (i.e., negligible loss and negligible number of hours of unplanned downtime).	The support PFS would suffer medium impact if IT systems were to be unavailable for an extended period.	The support PFS would suffer high impact if IT systems were to be unavailable for an extended period.	*Data are sensitive if being stolen, altered, or destroyed, it impacts business, compliance, or reputation*	The risk that performance and availability of ICT systems and data are adversely impacted, including the inability to timely recover the institution'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 (i.e., off the shelf or minimum customisation, no bug fixes required to fix unplanned outages caused by changes, no critical findings).	There is a limited frequency of significant changes to critical IT systems (i.e., low number of material change and no bug fixes 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.	*Data are sensitive if being stolen, altered, or destroyed, it impacts business, compliance, or reputation*	The risk arising from the inability of the institution 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 support PFS (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 (i.e., minor losses 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 support PFS.*	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.
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 (i.e., no invalid data modification, no cases of incorrect supervisory reporting data submitted, no critical finding).	Golden sources are defined but manual inputs and transfers are not fully under control (i.e., very low number invalid data modification and of known cases of incorrect supervisory reporting data submitted).	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 input.	*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 institution to provide services and produce (risk) management and financial information in a correct and timely manner.

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 ↓	Risk controls should be assessed by how effectively they mitigate 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.

Glossary

Term	Definition	Source
Administration system	IT administration systems (or IT management systems) are tools employed by organizations to configure, oversee, and control their Information Technology environment. These systems are designed to streamline and optimize the management of IT resources, ensuring the efficient operation of hardware, software, networks, and data. IT administration systems can be global (e.g., Management Plane) or dedicated to specific functions (e.g., Network Management, Server Management, User and Access Management, Security Management, Software Deployment and Patch Management, Asset Management, Backup and Recovery, Monitoring, and Reporting). This list of examples isn't exhaustive.	
Assessment of critical or important functions	Institutions must determine whether the function to be outsourced is considered critical or important (see definition of Critical or important function)	EBA/GL/2019/02
BIA (Business Impact Analysis)	The purpose of the BIA is to correlate specific IT components with the critical processes that they support and based on that information, to characterise the consequences of a disruption to the components. Results from the BIA should be appropriately incorporated into the analysis and strategy development efforts for the IT Disaster Recovery Plan, Business Recovery Plans, and the Incident Management Plan [NIST 800-34].	ENISA
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) or CSIRT (Computer Security Incident Response Team)	CERT/CSIRT has become a generic name for a team that provides a set of services: information and cybersecurity incident handling (core service), security monitoring, vulnerability management, situational awareness, and cybersecurity knowledge management. In simpler terms, a CERT/CSIRT is a team that is assigned to handle computer security (thus, often, cybersecurity) incidents. Often this includes additional responsibilities, from detection to analysis, and even hands-on fixing, as well as different situational awareness, knowledge transfer and vulnerability management activities. Over the years, the role of a CERT/CSIRT has evolved from providing incident monitoring and handling services to coordinating and communicating with different stakeholders, countries, and specific sectors.	ENISA
Client representative	Exclusively client representatives who have signed the contract and its potential amendments/addendum as well as further appendices with the support PFS.	
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/GL/2019/02
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).	
Crisis Incident Response Team	The Crisis Incident Response Team will be involved in the management of an incident if there is a need to call out the emergency services and/or initiate the crisis management. This team is generally composed of specific members designated before an incident and/or crisis occurs.	
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	A critical function is a business activity or process that must be restored in the event of a disruption to ensure the ability to protect the organization's assets, meet organizational needs, and satisfy regulations. In the context of outsourcing, according to section 4 of the EBA GLs on Outsourcing Arrangements, functions of which a defect or failure in 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
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.	
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

Term	Definition	Source
Data quality Management	This is to be understood as the management process to cover ICT data integrity risks as described in point 57 of the EBA Guidelines on ICT Risk Assessment under the SREP	EBA/GL/2017/05
Disaster Recovery Plan (DRP)	Documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster	
Disruption	An event which interrupts the ability of an organisation to deliver its output.	ENISA
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.	
Downtime	Downtime is the time in which a business function, a service and/or a specific IT-System is non-functional.	
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 developed applications are based on EXCEL or ACCESS files.	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.	
Financial sector clients	Credit institutions, PFS, payment institutions, electronic money institutions, UCIs, pension funds, SIFs, investment companies in risk capital, authorised securitisation undertakings, reserved alternative investment funds, insurance undertakings or reinsurance undertakings established under Luxembourg law or foreign law.	Law of 5 April 1993 on the financial sector
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 a 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 business lines, as part of the first line of defence, take risks and are responsible for their operational management directly and on a permanent basis. For that purpose, business lines should have appropriate processes and controls in place that aim to ensure that risks are identified, analysed, measured, monitored, managed, reported and kept within the limits of the institution's risk appetite and that the business activities are in compliance with external and internal requirements. Not only business lines, but also other functions or units, e.g., HR, legal or information technology, are responsible for managing their risks and having appropriate controls in place.	EBA/GL/2021/05
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 electronic retail payments that are processed in real time, 24 hours a day, 365 days a year, where the funds are made available immediately for use by the recipient. 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 Website
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/expenses 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.	

Term	Definition	Source
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
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. IT systems can encompass a wide range of network and system components, including servers, databases, software applications, operating systems, etc. (this list of examples isn't exhaustive). IT systems include IT administration systems.	EBA/GL/2017/05 (partially)
IT system related to client activities	IT system that partially or exclusively support the activities carried out for financial sector professional clients of the support PFS, irrespective of their belonging to the client of PFS or of their location and for which the support PFS is responsible as regards the sound functioning in relation to the client.	
Malware (malicious software)	The word Malware is derived from the term 'Malicious Software'. Any piece of software that performs undesirable operations such as data theft or some other type of computer compromise can be categorised as Malware. Malware is a broad term that can refer to various types of malicious programs. This document will cover some of the main types of Malwares, namely: Trojans, Viruses, Worms, and Spyware. The symptoms caused by these different types of malwares may sometimes be similar. However, they mainly differ in the way they spread and infect systems.	ENISA
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
Multi Factor Authentication	Multi-Factor Authentication (MFA) is a robust security protocol requiring users to authenticate their identity through the submission of two or more distinct verification factors. These factors align with the three foundational categories: - Something you know ("Knowledge-based factor"): This pertains to information known exclusively to the user, such as a password or PIN. - Something you have ("Possession-based factor"): This involves a tangible possession owned by the user, like an authenticated smartphone or computer, security token, or smart card. - Something you are ("Biometric factor"): This encompasses unique physiological or behavioural traits of the individual, such as fingerprints, facial features, or iris patterns. For instance, authentication with a user-specific password (knowledge-based factor) via the company computer assigned to the respective user (possession-based factor) already constitutes a 2FA authentication.	
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
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.	
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	
RPO (recovery point objective)	Point to which information used 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 independent control functions (e.g., IT risk, IT compliance), segregated by operations and business lines, that is responsible for monitoring and controlling adherence to the ICT and security risk management framework. It should ensure that ICT and security risks are identified, measured, assessed, managed, monitored, and reported.	EBA/GL/2019/04; EBA/GL/2021/05

Term	Definition	Source
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 security data from information system components and present that data as actionable information via a single interface.	NIST SP 800-128
Security Operations Centre (SOC)	A SOC, or security operations centre, provides an incident detection service by observing technical events in networks and systems and can also be responsible for incident response and handling. In large enterprises, SOCs sometimes focus only on monitoring and detection services and then hand over incident handling to a separate CSIRT. In smaller organisations, CSIRTs and SOCs are often considered to be synonymous.	ENISA
Service Provider	Service provider means a third-party entity that is undertaking an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement.	EBA/GL/2019/02
SSM Countries	All euro area countries participate automatically in European banking supervision. Other EU countries that do not yet have the euro as their currency can choose to participate. To do so, their national supervisors enter into “close cooperation” with the ECB. Bulgaria and Croatia joined European banking supervision through close cooperation in October 2020.	EZB
Supervisory Reporting	Supervisory reporting includes all the regular submission to the supervisor: COREP, FINREP, STE and STE-equivalent (as NPL reporting).	
Third Line of Defence	The third line of defence is internal audit, which provides independent assurance.	EBA/GL/2019/04; EBA/GL/2021/05