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

Section	Topic	Number	Questions	Test number	Test	Population for sample size purpose
Operational	**IT security management**	**Number**	**Questions**	**Test number**	**Test**	**Population for sample size purpose**
Operational	**Data Confidentiality**	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.	OPS-02.01	For a sample of IT systems (maximum 5 for support PFS classified as High Risk, maximum 3 for support PFS classified as Medium Risk or Low Risk by the CSSF) related to client activities, verify that **a review of logical accesses covering application users was performed during the year**.	Number of IT systems related to client activities.
				OPS-02.02	For the same sample as for the test OPS-02.01, verify that **a review of logical accesses covering high privileged users was performed during the year.**	
Operational	**Client activities**	**Number**	**Questions**	**Test number**	**Test**	**Population for sample size purpose**
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.	OPS-03.01	For a sample of procedures (maximum 3) related to client activities requiring a support PFS license, verify that data validation checks (e.g., 4 eyes principles) exist in the procedure or are enforced in the system.	Number of procedures related to activities which require a PFS authorization.
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.	OPS-05.01	For support PFS offering archiving services only: In case the archive recovery process is automated, reperform the archive recovery process for one document for one financial sector client contract and verify that the requested document is recovered in line with deadlines agreed within the contract. In case the archive recovery process is manual, for a sample of financial sector client contracts (maximum 3), reperform an archive recovery process and verify that the requested documents are recovered in line with deadlines agreed within the contracts.	In case the archive recovery process is manual, number of client contracts related to archiving activities which require a PFS authorization.

Transversal	IT continuity management	Number	Questions	Test number	Test	Population for sample size purpose
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.).	CROSS-01.01	Visit the locations related to client activities and identified as sensitive by the Support PFS (e.g. data centre/server rooms, archive rooms, print rooms) and observe that **multiple power sources or separate power substation are put in place.**	
				CROSS-01.02	Visit the locations related to client activities and identified as sensitive by the Support PFS (e.g. data centre/server rooms, archive rooms, print rooms) and observe that, **for data centre/server rooms**, **at least two diverse routes to telecommunication provider are put in place.**	
				CROSS-01.03	Visit the locations related to client activities and identified as sensitive by the Support PFS (e.g. data centre/server rooms, archive rooms, print rooms) and observe that, **for data centre/server rooms, a redundant air conditioning system is put in place.**	
				CROSS-01.04	Visit the locations related to client activities and identified as sensitive by the Support PFS (e.g. data centre/server rooms, archive rooms, print rooms) and observe that, **for data centre/server rooms, an UPS or equivalent is put in place.**	
				CROSS-01.05	Visit the locations related to client activities and identified as sensitive by the Support PFS (e.g. data centre/server rooms, archive rooms, print rooms) and observe that, for **data centre/server rooms, rack security locks or security slide bars are installed in shared areas/rooms.**	
				CROSS-01.06	Visit the locations related to client activities and identified as sensitive by the Support PFS (e.g. data centre/server rooms, archive rooms, print rooms) and observe that **all external doors and entries are protected.**	
				CROSS-01.07	Visit the locations related to client activities and identified as sensitive by the Support PFS (e.g. data centre/server rooms, archive rooms, print rooms) and observe that **temperature sensors are put in place.**	
				CROSS-01.08	Visit the locations related to client activities and identified as sensitive by the Support PFS (e.g. data centre/server rooms, archive rooms, print rooms) and observe that **humidity sensors are put in place.**	
				CROSS-01.09	Visit the locations related to client activities and identified as sensitive by the Support PFS (e.g. data centre/server rooms, archive rooms, print rooms) and observe that **flood or water overflow sensors are put in place.**	
				CROSS-01.10	Visit the locations related to client activities and identified as sensitive by the Support PFS (e.g. data centre/server rooms, archive rooms, print rooms) and observe that **smoke detectors are put in place.**	

Transversal	IT security management	Number	Questions	Test number	Test	Population for sample size purpose
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.	CROSS-02.01	For a sample of locations (maximum 3) related to client activities and identified as sensitive by the Support PFS (e.g. data centre/server rooms, archive rooms, print rooms), **for nominative badges (internal and external staff), confirm that they are allocated to active employees.**	Number of data centre/server rooms, archive rooms, print rooms and/or other locations related to client activities and identified as sensitive by the Support PFS.
				CROSS-02.02	For the same sample as for the test CROSS-02.01, **for generic badges (internal or external staff), confirm that users can be identified for the actions performed (e.g. in the badging systems) and that the process always allows accountability.**	
Transversal	**Data Confidentiality**	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.	CROSS-03.01	For a sample of data centre/server rooms and/or other locations (maximum 3) related to client activities and identified as sensitive by the Support PFS, verify that the support PFS has performed a review of the physical accesses during the year.	Number of data centre/server rooms, archive rooms, print rooms and/or other locations related to client activities and identified as sensitive by the Support PFS.

Transversal	Client activities	Number	Questions	Test number	Test	Population for sample size purpose
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.	CROSS-04.01	For a sample of clients (maximum 5 for support PFS classified as High Risk, maximum 3 for support PFS classified as Medium Risk or Low Risk by the CSSF), verify that **the report contains indications on availability**.	Number of client contracts related to activities which require a PFS authorization.
				CROSS-04.02	For the same sample as for the test CROSS-04.01, verify that **the report contains indications on quality of services (e.g., response time, error rate)**.	
				CROSS-04.03	For the same sample as for the test CROSS-04.01, verify that **the report contains information on incidents**.	
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.	CROSS-05.01	For a sample of client contracts related to activities which require a PFS authorization (maximum 5 for support PFS classified as High Risk, maximum 3 for support PFS classified as Medium Risk or Low Risk by the CSSF), verify that **the contract includes provisions on the possibility to sub-outsource (or not), in particular, a critical or important function, or material parts thereof.**	Number of client contracts related to activities which require a PFS authorization.
				CROSS-05.02	For the same sample as for the test CROSS-05.01, verify that **the contract includes provisions on the location(s) (i.e., regions or countries) where the function will be provided and/or where relevant data will be kept and processed.**	
				CROSS-05.03	For the same sample as for the test CROSS-05.01, verify that **the contract includes where relevant, provisions regarding the security of relevant data (e.g., the accessibility, availability, integrity, privacy and safety).**	
				CROSS-05.04	For the same sample as for the test CROSS-05.01, verify that **the contract includes provisions on the right of the client to monitor the support PFS's performance on an ongoing basis.**	
				CROSS-05.05	For the same sample as for the test CROSS-05.01, verify that **the contract includes provisions on the agreed service levels.**	
				CROSS-05.06	For the same sample as for the test CROSS-05.01, verify that **the contract includes provisions on the reporting obligations of the support PFS to its client (including the obligation to report any significant problem having an impact on the outsourced functions as well as any emergency situation).**	
				CROSS-05.07	For the same sample as for the test CROSS-05.01, verify that **the contract includes provisions on the requirements to implement and test business contingency plans.**	
				CROSS-05.08	For the same sample as for the test CROSS-05.01, verify that **the contract includes provisions on the unrestricted right of In-Scope Entities and competent authorities to inspect and audit the service provider, including in case of sub-outsourcing, with regard to, at least, the critical or important outsourced function.**	
				CROSS-05.09	For the same sample as for the test CROSS-05.01, verify that **the contract includes provisions on termination rights.**	
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.	CROSS-06.01	Verify the existence of a formalized emergency communication procedure.	

Transversal	Risk management	Number	Questions	Test number	Test	Population for sample size purpose
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).	CROSS-07.01	Verify the existence of a documented risk register.	
				CROSS-07.02	Verify that **the risk register contains a risk assessment for each risk.**	
				CROSS-07.03	Verify that **the risk register contains a risk response strategy for each risk.**	
				CROSS-07.04	Verify that **the risk register contains an action plan for each risk if relevant.**	
				CROSS-07.05	Verify that the risk register was last updated during the reference year.	

AML/CFT	Money laundering and terrorist financing risk	Number	Questions	Test number	Test	Population for sample size purpose
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.	AML-01.01	Inspect the policies and/or procedures regarding AML/CFT and international financial sanctions and verify that **they cover a risk-based approach.**	
				AML-01.02	Inspect the policies and/or procedures regarding AML/CFT and international financial sanctions and verify that **they cover customer due diligence measures.**	
				AML-01.03	Inspect the policies and/or procedures regarding AML/CFT and international financial sanctions and verify that **they cover higher risk customers requiring enhanced customer due diligence (e.g., Politically Exposed Persons (PEPs); High risk jurisdictions involved).**	
				AML-01.04	Inspect the policies and/or procedures regarding AML/CFT and international financial sanctions and verify that **they cover record keeping.**	
				AML-01.05	Inspect the policies and/or procedures regarding AML/CFT and international financial sanctions and verify that **they cover cooperation with the authorities.**	
				AML-01.06	Inspect the policies and/or procedures regarding AML/CFT and international financial sanctions and verify that **they cover name screening (international financial sanctions and PEPs).**	
				AML-01.07	Inspect the policies and/or procedures regarding AML/CFT and international financial sanctions and indicate **the date of the last review/update in the column "Brief description of deviations noted or explanation why test is not applicable".**	
				AML-01.08	Inspect the policies and/or procedures regarding AML/CFT and international financial sanctions and indicate **the date of the most recent approval in the column "Brief description of deviations noted or explanation why test is not applicable".**	
				AML-01.09	Inspect the policies and/or procedures regarding AML/CFT and international financial sanctions and indicate **the date of the most recent communication in the column "Brief description of deviations noted or explanation why test is not applicable".**	
AML/CFT	**ML and TF risk**	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).	AML-02.01	Obtain the list of all the financial sector clients of the support PFS and verify that a ML/TF risk level is allocated to each of them.	List of financial sector clients
AML/CFT	**Money laundering and terrorist financing risk**	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.	AML-03.01	Select a sample of the Support PFS' clients according to your (REA) ML/TF risk assessment of the Support PFS: - if you assessed the Support PFS as low risk, select 1 client file; - if you assessed the Support PFS as medium risk, select 2 client files; - if you assessed the Support PFS as high risk, select 3 client files. Inspect the KYC related documentation of the selected client files of the Support PFS and confirm that **the client's documentation available complies with the Support PFS AML/CFT policies and procedures.**	List of financial sector clients
				AML-03.02	For the same sample as for the test AML-03.01, inspect the KYC related documentation of the selected client files of the Support PFS and confirm that **the client's documentation available includes for lower risk clients, at least, a proof of their regulation, the identification of beneficial owners and representatives of the client, and an extract of the beneficial owner register (RBE).**	
				AML-03.03	For the same sample as for the test AML-03.01, ensure that **for high-risk clients, the periodic review has been performed at least every year, and for lower risk clients at least every 7 years.**	
AML/CFT	**Money laundering and terrorist financing risk**	AML-05	The support PFS has an automated *name screening* system or performs the screening manually.	AML-05.01	For the same sample as for the test AML-03.01, verify (by observing) that **the clients, their beneficial owners and representatives are encoded/listed in the support PFS client database or documentation (i.e., the one screened against international financial sanctions list).**	List of financial sector clients
				AML-05.02	When an automated system is used, choose the name of 2 legal or natural persons from international financial lists (i.e., UE, UN or Luxembourg lists) and check that these 2 names produce an alert in the Support PFS screening system.	
AML/CFT	**Money laundering and terrorist financing risk**	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)	AML-06.01	Confirm that the Support PSF is able to connect the goAML web platform.	

Sample size instructions

Use these sample size instructions when the test description does not provide any indication.

Sample size instructions	
Population size*	**Sample size**
1 to 3	1
4 to 11	2
12 to 50	4
50-300	10% (i.e., 5 to 30)
More than 300	30

** Population is defined for each procedure*