Separate Report - Art. 29-3, 29-5 & 29-6 of the LFS – Medium Risk

Section	Topic	Number	Questions	Rotation Year	Test number	Test	Population for sample size purpose
ICT	**IT security management**	**Number**	**Questions**	**Rotation Year**	**Test number**	**Test**	**Population for sample size purpose**
ICT - Medium Risk	**Security reviews**	ICT-12	Security reviews on the general information security controls, processes and procedures are carried out regularly.	Year 2	ICT-12.01	Inspect a sample of penetration testing report(s) performed within the reference year, and confirm that for **the 5 most important** findings **(for each penetration testing report tested),** action plans have been formalized **(all findings if a sampled report contains less than 5 findings)**.	Number of penetration testing report(s) performed within the reference year.
				Year 2	ICT-12.02	For the same sample as for the test ICT-12.01, confirm that for the 5 most important findings (for each penetration testing report tested), action plans include a defined timeframe.	
ICT - Low Risk	**Identity and access management**	ICT-15	A documented user access management procedure (covering all accounts including privileged accounts) approved by the management is developed, implemented, enforced, duly monitored and reviewed and in line with information risk management requirements.	Year 1	ICT-15.01	**Access provision:** 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, inspect relevant documentation for a sample of new joiners and movers (within internal and external Support PFS personnel) within the reference year to confirm that accesses were provisioned in line with the access management procedure.	Number of IT systems related to client activities. Number of new accesses (including contractors) during the reference period.
				Year 1	ICT-15.02	**Access removal:** 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, inspect relevant documentation for a sample of leavers and movers (within internal and external Support PFS personnel) within the reference year to confirm that accesses were removed in line with the access management procedure.	
ICT - Medium Risk	**Identity and access management**	ICT-16	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.	Year 2	ICT-16.01	For a sample of IT systems (maximum 5 for support PFS classified as High Risk, maximum 3 for support PFS classified as Medium Risk by the CSSF) related to client activities, inspect the list of all accounts belonging to the Support PFS (including privileged, generic and service accounts), **for nominative end-user accounts (internal and external staff), confirm for a sample of accounts that they are allocated to active employees.**	Number of IT systems related to client activities. Number of nominative end-user accounts.
				Year 2	ICT-16.02	For the same sample as for the test ICT-16.01, **for nominative (non-generic) privileged accounts (internal and external staff), confirm that they are limited and granted in accordance with the principle of the least privilege.**	
				Year 2	ICT-16.03	For the same sample as for the test ICT-16.01**, for generic privileged accounts, confirm that users can be identified for the actions performed in the IT systems, i.e., always allows accountability (e.g., using a Privileged Access Management (PAM) solution).**	
				Year 2	ICT-16.04	For the same sample as for the test ICT-16.01, **for technical accounts (used by systems for automated processing purposes such as batch, back-up, connectivity), confirm that access is limited (e.g., employees are technically unable to use these accounts, the passwords for these accounts are securely stored and access to them is restricted).**	
ICT - Low Risk	**Identity and access management**	ICT-17	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.	Year 1	ICT-17.01	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.
				Year 1	ICT-17.02	For the same sample as for the test ICT-17.01, verify that **a review of logical accesses covering high privileged users was performed during the year.**	

ICT	IT security management	Number	Questions	Rotation Year	Test number	Test	Population for sample size purpose
ICT - Low Risk	**Identity and access management**	ICT-18	Multi-Factor Authentication (MFA) is used when accessing administration systems and access to sensitive information. The strength of authentication is appropriate for the classification of the asset to be accessed.	Year 1	ICT-18.01	For a sample of administration 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 and including those containing sensitive information, inspect the access mechanism and confirm that Multi-Factor Authentication (MFA) is in place.	Number of administration systems related to client activities.
ICT - Medium Risk	**Identity and access management**	ICT-19	The support PFS maintains a documented, approved and enforced logging and monitoring procedures, which covers in particular the logs of actions performed by privileged accounts and the log retention period. Logs are secured to prevent unauthorised modification or deletion and retained for a period commensurate with the criticality of the identified business functions, and client requirements.	Year 2	ICT-19.01	Inspect the logging and monitoring procedures and confirm that **the procedures were documented and approved.**	
				Year 2	ICT-19.02	Inspect the logging and monitoring procedures and confirm that **the procedures cover the logging of actions performed by privileged accounts.**	
				Year 2	ICT-19.03	Inspect the logging and monitoring procedures and confirm that **the procedures cover the log retention period(s).**	
				Year 2	ICT-19.04	Inspect the relevant documentation (e.g., configuration, access rights, etc.) and confirm that, for a sample of IT systems (maximum 5 for support PFS classified as High Risk, maximum 3 for support PFS classified as Medium Risk by the CSSF) supporting client activities, logs are secured to prevent unauthorised modification or deletion.	Number of IT systems related to client activities.
ICT - Low Risk	**Patch and vulnerability management**	ICT-20	Patch and vulnerability management is developed and implemented. Vulnerability management process covers all IT assets. The patches are deployed in a timely manner according to their criticality or compensating controls are implemented in a timely manner.	Year 1	ICT-20.01	Inspect the status of the patch deployment 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 and confirm that **the status is up-to-date.**	Number of IT systems related to client activities. Number of vulnerability scanning reports.
				Year 1	ICT-20.02	For the same sample as for the test above, **in case patches have not been deployed, check the existence of formalized and approved justifications.**	
				Year 1	ICT-20.03	Inspect 5 vulnerability scanning reports related to IT systems related to client activities, and confirm that the 5 most important vulnerabilities **(for each vulnerability scanning report tested)** were mitigated in a timely manner.	
ICT - Medium Risk	**Network security (incl. remote access)**	ICT-23	Remote access to systems is controlled through secure authentication methods like Multi-Factor Authentication (MFA) and Virtual Private Networks (VPNs).	Year 2	ICT-23.01	For a sample of IT systems (maximum 5 for support PFS classified as High Risk, maximum 3 for support PFS classified as Medium Risk) related to client activities, observe remote authentication and confirm that remote access is controlled through secure authentication methods like Multi-Factor Authentication (MFA) and Virtual Private Networks (VPNs).	Number of IT systems related to client activities.
ICT - Medium Risk	**Security event logging & monitoring**	ICT-24	The support PFS has implemented effective measures to log, monitor and analyse security events and promptly react in case of alerts within timelines defined in a dedicated procedure.	Year 2	ICT-24.01	Based on the list of all security alerts/events logged, for a sample of security events with highest level of criticality (based on the entity's criticality scale), inspect relevant documentation and confirm that **the events were documented**.	Number of security alerts/events (incl. Physical security) with the highest level criticality logged and monitored.
				Year 2	ICT-24.02	For the same sample as for the test ICT-24.01, inspect relevant documentation and confirm that **the events documented were addressed according to deadlines defined in the procedures**.	

ICT	IT operations management	Number	Questions	Rotation Year	Test number	Test	Population for sample size purpose
ICT - Low Risk	**Asset inventory and configuration management**	ICT-28	The support PFS maintains an updated inventory of its ICT assets, including IT systems and applications, in order to ensure a proper configuration, change and incident management.	Year 1	ICT-28.01	Inspect the inventory of all ICT assets, including IT systems and applications related to client activities, and confirm that the last update was performed at least once within the reference period.	
				Year 1	ICT-28.02	For a sample of ICT assets related to client activities, inspect the inventory and confirm that **each asset has a unique identifier.**	Number of ICT assets related to client activities.
				Year 1	ICT-28.03	For the same sample as for the test ICT-28.02, confirm that **the inventory contains the asset type** (e.g., server, software application, network device).	
				Year 1	ICT-28.04	For the same sample as for the test ICT-28.02, confirm that **the inventory contains the version/release** (For software and applications).	
				Year 1	ICT-28.05	For the same sample as for the test ICT-28.02, confirm that **the inventory contains the physical location** (e.g., DC name or cloud region).	
				Year 1	ICT-28.06	For the same sample as for the test ICT-28.02, confirm that **the inventory contains the current status** (active, inactive, or in maintenance mode).	
				Year 1	ICT-28.07	For the same sample as for the test ICT-28.02, confirm that **the inventory indicates the environment of the assets (test, dev, prod).**	
				Year 1	ICT-28.08	For the same sample as for the test ICT-28.02, confirm that **the inventory contains the asset classification by importance** (e.g., criticality level) or by security objectives (e.g., confidentiality, integrity, availability).	
				Year 1	ICT-28.09	For the same sample as for the test ICT-28.02, confirm that **the inventory indicates the links/interdependencies of the assets with other ICT assets.**	
ICT - Low Risk	**Backups**	ICT-31	The support PFS backs up the clients' hosted IT systems in line with clients requirements as defined in the contractual agreements.	Year 1	ICT-31.01	For a sample of clients for whom backup services are offered (maximum 2 for support PFS classified as High Risk, maximum 1 for support PFS classified as Medium Risk or Low Risk by the CSSF), obtain a list of the IT systems associated with the client's activities. For a sample of these systems (maximum 3) inspect the backup execution report for a sample of days/weeks/months (depending on the defined backup frequency) and confirm that **the backups were executed in compliance with the clients' requirements related to frequency and nature (incremental or full) as defined in the contractual agreements.**	Number of clients for whom backup services are offered. Number of IT systems related to these clients' activities. Number of days/weeks/months (depending on the defined backup frequency).
				Year 1	ICT-31.02	For the same sample as for the test ICT-31.01, confirm that, **according to the backup execution report, the backup was run successfully.**	
ICT - Low Risk	**IT operations (incl. job scheduling, system monitoring, capacity management…)**	ICT-33	The support PFS has documented and implemented procedures to ensure the standard operations of the IT systems. Such procedures cover at least: * The job scheduling process; * The monitoring of IT systems (systems are monitored at all times and automatic alerts are sent to dedicated teams ensuring continuous operations); * The capacity management to ensure system resources (e. g. CPU, RAM, Hard Disk space ...) are always in line with the application needs and can cope with performance peaks; * Maintenance and repair of the assets; and * Shift handover (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.	Year 1	ICT-33.01	For a selection of days, inspect the job scheduling logs (whether via manual checklists or via an automated system) and confirm that **operations of IT systems related to client activities are covered (including proper start, execution, end of tasks, adequate capacity, disk space, etc.).**	Number of days in the reference period (year)
				Year 1	ICT-33.02	For the same sample as for the test ICT-33.01, confirm that **alerts related to events or job failures are logged**.	
				Year 1	ICT-33.03	For the same sample as for the test ICT-33.01, confirm that **alerts related to events or job failures are followed up.**	

ICT	IT continuity management	Number	Questions	Rotation Year	Test number	Test	Population for sample size purpose
ICT - Medium Risk	**IT continuity and disaster recovery - plans, processes and procedures**	ICT-41	The support PFS has an appropriately documented crisis management framework in place and regularly reviews plans, processes and procedures to enable the continuity and recovery of IT systems related to client activities (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.). The RPO and RTO have been defined factoring in those agreed with the clients.	Year 2	ICT-41.01	Inspect the plan(s) related to continuity and recovery management of IT systems and services related to client activities (including outsourced systems and services) and confirm that **they are documented.**	
				Year 2	ICT-41.02	Inspect the same plans as for the test above and confirm that **they are regularly (at least once a year) reviewed and updated.**	
				Year 2	ICT-41.03	Inspect the same plans as for the test above and confirm that **updates are approved.**	
				Year 2	ICT-41.04	Inspect the same plans as for the test above and confirm that **they have been built considering extreme but plausible (according to the support PFS) scenarios to which the support PFS might be exposed, including cyber-attacks, third-party dependencies.**	
				Year 2	ICT-41.05	Inspect the same plans as for the test above and confirm that **they have been built based on a Business Impact Analysis (BIA).**	
				Year 2	ICT-41.06	Inspect the same plans as for the test above and confirm that **they contain formalised RPO and RTO.**	
ICT - Low Risk	**IT continuity and disaster recovery - testing & continuous improvement**	ICT-43	For IT systems related to client activities, where the criticality is expected to be adequately reflected in frequency (at least once a year), and taking into account a range of realistic scenarios, the support PFS regularly and sufficiently tests its business continuity plans, disaster recovery plans and essential protective measures to assess their usefulness and reliability.	Year 1	ICT-43.01	Confirm that business continuity plans and disaster recovery plans **tests have been performed at least once during the reference period for critical IT services offered to financial sector clients, supporting processes, assets and, if any, third parties.**	
				Year 1	ICT-43.02	Confirm that business continuity plans and disaster recovery plans **tests include the switch-over for critical IT services offered to financial sector clients, supporting processes, assets and, if any, third parties.**	

Transversal	IT security management	Number	Questions	Rotation Year	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.	Year 2	CROSS-02.01	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, **for nominative badges (internal and external staff), confirm that they are allocated to active employees.**	Number of data centre/server rooms and/or other locations related to client activities and identified as sensitive by the Support PFS.
				Year 2	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.	Year 2	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 and/or other locations related to client activities and identified as sensitive by the Support PFS.

Transversal	Client activities	Number	Questions	Rotation Year	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.	Year 2	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.
				Year 2	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)**.	
				Year 2	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.	Year 2	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.
				Year 2	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.**	
				Year 2	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).**	
				Year 2	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.**	
				Year 2	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.**	
				Year 2	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).**	
				Year 2	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.**	
				Year 2	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.**	
				Year 2	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.	Year 2	CROSS-06.01	Verify the existence of a formalized emergency communication procedure.	

Transversal	Risk management	Number	Questionsp	Rotation Year	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).	Year 2	CROSS-07.01	Verify the existence of a documented risk register.	
				Year 2	CROSS-07.02	Verify that **the risk register contains a risk assessment for each risk.**	
				Year 2	CROSS-07.03	Verify that **the risk register contains a risk response strategy for each risk.**	
				Year 2	CROSS-07.04	Verify that **the risk register contains an action plan for each risk if relevant.**	
				Year 2	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	Rotation Year	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.	Each year	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.**	
				Each year	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.**	
				Each year	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).**	
				Each year	AML-01.04	Inspect the policies and/or procedures regarding AML/CFT and international financial sanctions and verify that **they cover record keeping.**	
				Each year	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.**	
				Each year	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).**	
				Each year	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".**	
				Each year	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".**	
				Each year	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).	Each year	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.	Each year	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
				Each year	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).**	
				Each year	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.	Each year	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
				Each year	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)	Each year	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*