Category	Data Points under Art. 12 (7) AMLAR and Art. 40 (2) AMLD	Answer
1 - Governance, Culture & Compliance function (Role and responsibilities of the management body, AML/CFT risk culture, AML/CFT Compliance Function and Resources, AML/CFT training)	Date at which the procedures covering the entirety of the AML/CFT framework (including initial and ongoing CDD, transaction and business relationship monitoring, STR, and financial sanction screening) were checked as being in compliance with existing laws and regulations applicable at that date	
	Number of dedicated AML/CFT compliance staff (in FTE)	
	% of personnel per category who have received AML training during the last calendar year:	
	a) AML/CFT compliance staff	
	b) non-AML/CFT compliance staff (e.g. customer facing staff)	
	c) agents and distributors	
	d) Board members / non-executive directors	
2 - Internal Controls & Outsourcing (Internal controls and reporting systems, Outsourcing and reliance on third parties, Internal audit function / external expert, Record keeping)	Frequency of reporting by the AML compliance officer to the management body (never, monthly, quarterly, half-yearly, yearly)	
	Tasks outsourced by the credit institution or financial institution (in total or in part) to service providers:	
	CDD	
	Training	
	Transaction Monitoring	
	Suspicious Transaction Reports	
	Sanctions Screening	
	PEP detection	
	Compliance Monitoring Checks	
	AML/CFT tasks outsourced to an external service provider located in third country that is not part of the group (Y/N)	
	Existence of AML/CFT tasks outsourced to an external service provider located in third country that is part of the group (Y/N)	
	Dates when the AML/CFT obligations/ controls were last assessed by an internal/external audit:	
	a. BWRA	
	b. determination of ML/TF risk profile of customers in a business relationship	
	c. AML/CFT-related awareness-raising and staff training measures	
	d. Identification and identity verification procedures	
	e. Policies and procedures for monitoring and analysing business relationships, including transaction monitoring	
	f. Policies and procedures for suspicious transaction reporting	
	g. Record keeping policies and procedures	
	h. Resources dedicated to AML/CFT	
	i. Organisation of the AML/CFT system, governance and reporting to management bodies.	
3 - Risk assessment (Business Wide Risk Assessment (BWRA) and Customer ML/TF risk assessment and classification (CRA))	Last approval date of the BWRA	
	Senior management approved the last version of the BWRA (Y/N)	
	Date of the last update of the CRA	
	Number of customers per ML/TF risk category (low risk, medium-low risk, medium-high risk, high-risk)	
4 - Customer due diligence & monitoring (Customer Due Diligence and Ongoing monitoring of business relationships)	Number of customers that are legal entities /trusts whose beneficial owners have not been identified	
	Number of customers that are legal entities /trusts whose beneficial ownership has been identified, but the identity of whom has not been verified	
	Number of customers without identification and verification documentation/ information	
	Number of customers whose CDD data and information is not yet in line with the requirements of Article 20 AMLR	
	Number of customers without ML/TF risk profile (excluding customers with whom the credit institution or financial institution does not have a business relationship)	
	Number of customers for whom updates of customer information were due in the last calendar year, in accordance with the credit institution or financial institution 's policies and procedures	
	Number of customers for whom customer information was reviewed and updated in the last calendar year	
5 - Transaction monitoring and Suspicious Activity Reporting	The credit institution or financial institution has a transaction monitoring system in place (Y/N)	
	The transaction monitoring system is:	
	a) Not automated; or	
	b) At least partly automated	
	If manual system: Average time in days to analyse the transaction since the moment it occurred	
	If automated system: The system can generate alerts in case of inconsistencies between CDD information relating to the customer and the following elements:	
	a) Number of transactions	
	b) Value of aggregated transactions	
	c) value of single transactions	
	d) counterparties	
	e) countries	
	If automated system: Number of alerts not analysed at the end of the calendar year	
	If automated system: Average time to analyse an alert in the last calendar year (number of days between that the alert was generated and the moment that the alert was closed)	
	If automated system: Ratio between number of alerts and number of STRs	
	The entity has implemented a tool that enables it to analyse the information available on distributed ledgers and generate alerts where unusual patterns or risk factors are identified, in relation to the transactions carried out by the customer (Y/N)	
	Average number of days between the date of identification of potential suspicious transactions (prior to the analysis of the transaction) and the date when the transaction is reported to the FIU (after the analysis of the transaction) during the last calendar year	
	Total number of STRs submitted to the FIU during the last calendar year	

Category	Data Points under Art. 12 (7) AMLAR and Art. 40 (2) AMLD	Answer
6 - Targeted Financial Sanctions and Compliance with Fund Transfers Regulation	Maximum number of hours between the publication of the TFS by the authorities and the implementation of these changes in the institution's screening tools	
	Number of outbound transfers for which requests were received from a counterparty in the transfer chain for information that is missing, incomplete or provided using inadmissible characters in the last calendar year	
	Total number of outbound transfers in the last calendar year	
	% of outbound transfers rejected or returned by the counterparty in the transfer chain due to information that is missing, incomplete or provided using inadmissible characters in the last calendar year	
7 - Group-wide AML/CFT Framework (AML/CFT governance structures, Group-wide ML/F risk assessment, Group policies and procedures, including sharing of information, Group-wide AML/CFT function)	% of group entities that provided reports to the Group AML compliance on the following areas in the last calendar year (should only be answered by the parent company):	
	a) CDD	
	b) ongoing monitoring	
	c) STRs	
	d) identity and transaction level information on high risk customers	
	e) deficiencies	
	% of jurisdictions in which the group is established covered by reviews (including access to customer and transaction level data) performed by the group AML/CFT compliance function in the last three calendar years. (applies only to groups that have been existing for more than 3 years and should only be filled in by the parent company)	
	Number of group entities for which deficiencies were identified by competent AML/CFT supervisors in the last calendar year (should only be filled in by the parent company)	
	- EU/EEA entities	
	- Non-EU/EEA	