# Example FI Anti-Money Laundering (AML)/Counter Financing of Terrorism (CFT) Policy

| | AML/CFT Policy structure |
|---|---|
| 1 | **Introduction & Policy Statement** - Set out the FI's stance or position on AML/CFT typically referring to legal or regulatory obligations (including tipping-off provisions) to comply with and the firm's commitment to adherence to relevant legislation (list e.g. UK Money Laundering, Proceeds of Crime Act 2002, Terrorist Financing & Transfer of Funds Regulations 2017) |
| 2 | **Define Money Laundering** (including the three-stage process of placement, layering and integration) and why money laundering is important to combat and penalties/reputational risk for non-compliance (FI, Directors, Employees). |
| 3 | **Define Terrorist Financing and** difference between ML and TF and why TF is important to combat and penalties/reputational risk for non-compliance (FI, Directors, Employees). |
| 4 | **Economic Sanctions** include what are economic sanctions and governments/supranatural bodies implementing sanctions e.g. UN to achieve specific objectives such as countering criminal activity and human rights abuses. Outline restrictions imposed by sanctions including freezing of assets of entities and individuals and extraterritoriality of some sanctions regimes including the US. Refer to all employees needing to comply with relevant sanctions laws including compliance by US persons to US sanctions |
| 5 | **Outline typical red flags for Money Laundering/Terrorist Financing.** Examples include:<br>• Customers being secretive about who they are or reason for the transaction or refusing to provide relevant documentation<br>• Unusual or unexpected transactions for the customers profile e.g. unexplained payments from foreign countries or third parties<br>• Large or multiple cash payments |
| 6 | **Internal Compliance structure to manage Money Laundering or Terrorist Financing**<br>Outline responsibilities of AML/CFT compliance function and organogram including duties of MLRO/Compliance Officer with respect to AML/CFT |
| 7 | **Risk-based Approach**<br>Outline FIs risk assessment approach to AML/CFT including identification and evaluation of risks associated with customers, products, services, delivery channels and geographies for different businesses (e.g. retail, wealth management, trade finance, investment banking, correspondent banking). Based on the risk assessment classify customers as low, medium, high risk (or low/high) for standard or enhanced customer due diligence and associated monitoring requirements.<br><br>Outline exclusions including Shell Banks, fictitious customers or customers where there are suspicions of ML/TF or the request for funds doesn't make sense or align with the customers activity. |

| | |
|---|---|
| **8** | **Customer Due Diligence (including KYC)**<br>Know Your Customer (KYC) - Outline the process for identifying and verifying customers, beneficial owners, authorized signatories, and key controllers alongside verifying if the customers request for funds, profile and business activity makes sense. KYC requirements should be set out for: individual customers; sole proprietors; partnerships; private limited companies; public limited companies and Societies, NGO, trusts & charities (where applicable).<br><br>Set out conducting standard and enhanced due diligence on customers.<br><br>The FI should conduct CDD that includes all the relevant risk factors (for example, geography, product usage, industry, legal entity type, and customer screening results e.g. negative media checks). A process should be in place for periodically updating customer information e.g. higher-risk customers reviewed every year, Medium-and lower-risk customers every 2–5 years or based on a trigger event. Politically Exposed Persons should be defined and classified as high risk with procedures to undertake source of funds and wealth checks outlined.<br><br>Based on the AML/CFT risk assessment, the FI should conduct terrorist/sanctions, negative news, and PEP screening at customer onboarding and on a frequent basis thereafter (for example, daily or weekly). Potential matches should be promptly reviewed and escalated for review to determine if action required e.g. notification of suspicious activity to the regulator. |
| **9** | **Transaction Monitoring (where relevant)**<br>Outline how customer accounts are monitored to identify unusual/potentially suspicious activity by a transaction monitoring solution or through other means including how hits are reviewed, investigated, and, if applicable, escalated within a prescribed time frame (for example, 24 hours). All activity determined to be suspicious should be reviewed by a senior compliance person (and/or a suspicious transaction report review committee). |
| **10** | **Reporting (including suspicious transaction/activity reporting)**<br>Outline regular management reporting covering all the relevant AML/CFT areas (for example, risk assessment, high-risk customers, suspicious transaction reports, transaction monitoring alerts, and customers with outstanding EDD/CDD/identification verifications). The reports are made available to all relevant stakeholders from the board of directors and senior management to operational management on a frequent basis (for example, monthly or quarterly). The FI should have formal processes in place to track, monitor, and report on special projects related to AML/CFT compliance (for example, elimination of backlog or KYC remediation).<br><br>All identified unusual/ suspicious transactions should be reported in a timely manner to the respective supervisory body. All STRs should be reviewed by a senior compliance person. |
| **11** | **Managing Law enforcement enquiries**<br>Any requests from law enforcement e.g. courts or police should be reviewed and completed by a senior compliance person. e.g. MLRO. This includes Information or Production Orders |
| **12** | **Record Keeping**<br>Documents and records pertaining to AML/CFT compliance e.g. CDD/KYC records and STRs should be retained by the bank for the required period stipulated by the regulator and properly destroyed at the end of the retention period. All records must be maintained |

| | |
|---|---|
| | in a formal/depository that can be accessible for access by the compliance team, internal audit or the regulator. |
| **13** | **Communication & Training**<br>The FI should provide mandatory AML/CFT training to all employees regularly (e.g. annually) alongside targeted detailed training to specific roles e.g. compliance and due diligence teams. Training should be provided to new hires.<br><br>Records of training are maintained. |
| **14** | **Continuous Improvement & testing**<br>The bank's AML/CFT compliance department should test/conduct quality assurance of all the relevant AML/CFT processes (for example, CDD, STR reporting, cash transaction reporting, and training). Testing/quality assurance should be performed on a frequent basis (quarterly), and such requirement is documented in the bank's policies and procedures.<br><br>The FIs internal audit function (or an external audit provider) should also conduct independent testing on AML/CFT controls on annual basis. Audit results are shared with the board, senior management, and the AML/CFT officer. Where deficiencies are identified, a formal action plan is developed, and the progress on the action plan is reported to senior management on a regular basis. These requirements are documented in the bank's policies and procedures.<br><br>The internal audit department should be independent and have sufficient authority to perform their responsibilities with objectivity. All their recommendations should be implemented by appropriate departments in a timely manner. |