AML/CFT Program

Compliance Program | Global

Version 2.0 · July 2026 · Confidential — Internal Use

This document is a template intended to be reviewed, tailored and approved by your organisation before use.
Replace all references to “the Company” with your organisation’s name.

Document Control

Document name	AML/CFT Program
Document type	Compliance Program
Jurisdiction	Global
Owner	Chief Compliance Officer / AML/CFT Compliance Officer
Approved by	Board of Directors
Version	2.0
Effective date	July 2026
Review cycle	Annual
Next review due	July 2027
Classification	Confidential — Internal Use

Contents

1. Purpose
2. Scope
3. Definitions
4. Regulatory Framework
5. Policy Statement and Program Structure
6. Enterprise ML/TF and PF Risk Assessment
7. Governance, Oversight and Accountability
8. Risk-Based Controls and Customer Due Diligence
9. Sanctions, PEP and Adverse Media Screening
10. Transaction Monitoring Program
11. FIU Reporting and Record Keeping
12. Employee Due Diligence and Training
13. Independent Review and Assurance
14. Breaches, Escalation and Review of this Program
Appendix A: Program and Risk Assessment Review Trigger Events
Appendix B: FIU and Regulatory Reporting Obligations Summary
Policy Administration

1. Purpose

This document is the Company's AML/CFT Program. It sets out how the Company identifies, assesses, mitigates and manages the risk that its products, services, transactions, channels and relationships might involve or facilitate money laundering (ML), terrorism financing (TF) or proliferation financing (PF), and how the Company complies with the anti-money laundering and counter-financing of terrorism laws applicable in each jurisdiction in which it operates. The Program is anchored to the FATF Recommendations, the Basel Committee's guidelines on the sound management of ML/FT risks and the standards of the Wolfsberg Group.

The Program documents the Company's enterprise ML/TF/PF risk assessment methodology and the policies, systems and controls that respond to the assessed risks: governance and oversight arrangements, risk-based customer controls, sanctions and PEP screening, transaction monitoring, suspicious transaction reporting to the financial intelligence unit (FIU), employee due diligence, training, independent review and record keeping. Detailed customer identification, verification, beneficial ownership and ongoing due diligence procedures are set out in the companion Customer Due Diligence (KYC) Program, which forms part of the Company's AML/CFT framework and is to be read together with this document.

This Program is made under the authority of, and is approved by, the Board of Directors. The Chief Compliance Officer, as the appointed AML/CFT Compliance Officer, is responsible for preparing, maintaining and reviewing the Program. The Program gives effect to the Board's determination that the Company will not tolerate its products, services or channels being used to facilitate financial crime.

2. Scope

This Program applies to the Company and to every subsidiary, branch and other controlled entity of the Company, in every jurisdiction in which the Company operates. Consistent with the FATF group-wide programme requirement, foreign branches and majority-owned subsidiaries must apply this Program; where the law of a host jurisdiction prevents full application, the AML/CFT Compliance Officer must document the conflict, determine and implement appropriate additional measures, and notify the home supervisor within [20] business days. The [Board Risk Committee] must decide, within [60] days of notification, whether the residual exposure is within the Board-approved risk appetite; where it is not, or where the additional measures are insufficient, the Board must decide whether the Company will restrict or cease the affected products, services or operations in that jurisdiction. Each such determination and the supporting analysis must be recorded by the AML/CFT Compliance Officer and reviewed at least annually.

The Program binds all directors, officers, employees, secondees, contractors and agents of the Company, and applies to all products and services offered by the Company, all customer segments, all delivery channels (branch, broker and intermediary, digital, telephone and correspondent) and all jurisdictions with which the Company deals through customers, transactions, correspondents, group entities or service providers.

- Customer identification, verification, beneficial ownership and ongoing due diligence procedures are set out in the Customer Due Diligence (KYC) Program.
- Detailed sanctions screening, hit management and asset freezing requirements are set out in the Sanctions Policy; this Program addresses sanctions only as a control supporting the management of ML/TF/PF risk.
- Operational procedures, monitoring rule libraries and work instructions that implement this Program are maintained by the AML/CFT Compliance Officer and listed in the AML/CFT document register.

2.1 Jurisdictional application

This Program states international best practice by reference to the FATF Recommendations and related standards. The Company must map every requirement in this Program to the AML/CFT law of each jurisdiction in which it operates — including licensing and registration, reporting types and deadlines, thresholds, retention periods and tipping off provisions — and complete every bracketed placeholder from those laws. Where the law of an operating jurisdiction imposes a stricter or additional requirement, local law prevails and must be complied with.

3. Definitions

Term	Definition
AML/CFT Compliance Officer	The person appointed by the Board at senior management level, assessed as fit and proper, who is responsible for oversight of the day-to-day operation of this Program and for liaison with the financial intelligence unit and other competent authorities.
Beneficial Owner	The natural person or persons who ultimately own or control a customer, directly or indirectly, including through holding [25]% or more of the ownership interests or voting rights (or any lower threshold prescribed by applicable local law), any person who otherwise exercises ultimate effective control over the customer, and any person on whose behalf a transaction is conducted.
Customer Due Diligence (CDD)	The measures by which the Company identifies a customer and verifies its identity using reliable and independent sources, identifies and takes reasonable measures to verify beneficial owners,

	understands the ownership and control structure and the purpose and intended nature of the business relationship, and keeps that understanding current through ongoing monitoring, consistent with FATF Recommendation 10.
Enhanced Due Diligence (EDD)	More intensive due diligence measures applied beyond the standard requirements where the money laundering, terrorism financing or proliferation financing risk of a customer, counterparty, transaction, relationship or other party is assessed as high, or where a mandatory trigger arises, including additional verification, establishment of source of funds and source of wealth, senior management approval and enhanced ongoing monitoring.
Financial Intelligence Unit (FIU)	The national agency in each jurisdiction in which the Company operates that acts as the central authority for receiving, analysing and disseminating suspicious transaction reports and other information relevant to money laundering, associated predicate offences, terrorism financing and proliferation financing, consistent with the FATF Recommendations.
ML/TF/PF Risk	The risk that the Company may reasonably face that the provision of its products and services might, whether inadvertently or otherwise, involve or facilitate money laundering, terrorism financing or proliferation financing.
Money Laundering (ML)	The process of concealing or disguising the criminal origin of funds or other assets, including their conversion, transfer, acquisition, possession or use, so that they appear to derive from a legitimate source.
Ongoing Due Diligence	The continuing process of monitoring customers and their transactions, and of reviewing and updating know-your-customer and beneficial ownership information, so that customer risk ratings and controls remain appropriate throughout the relationship.
Politically Exposed Person (PEP)	An individual who is or has been entrusted with a prominent public function, whether domestically, in a foreign country or by an international organisation, together with that individual's immediate family

	members and close associates, classified as domestic, foreign or international organisation PEPs consistent with the FATF standards.
Proliferation Financing (PF)	The provision of funds or financial services used, in whole or in part, for the manufacture, acquisition, development, export or transport of nuclear, chemical or biological weapons or their means of delivery, including in breach of targeted financial sanctions.
Risk-Based Approach	The approach required by the FATF Recommendations under which the Company identifies, assesses and understands its ML/TF/PF risks and applies controls whose intensity is proportionate to those risks.
Shell Bank	A bank that has no physical presence in the country in which it is incorporated and licensed, and that is not affiliated with a regulated financial group subject to effective consolidated supervision.
Suspicious Transaction Report (STR)	A report submitted to the FIU, however styled in the relevant jurisdiction and including a suspicious activity report (SAR), where the Company suspects or has reasonable grounds to suspect that funds or activity are the proceeds of criminal conduct, including fraud, or are related to terrorism or proliferation financing, consistent with FATF Recommendation 20.
Targeted Financial Sanctions	Asset-freezing measures and prohibitions on making funds or other assets available, directly or indirectly, to or for the benefit of specifically designated persons and entities, as required by United Nations Security Council resolutions, reflected in FATF Recommendations 6 and 7, and imposed under applicable autonomous sanctions regimes.
Tipping Off	The prohibited disclosure to a customer or any other unauthorised person that a suspicious transaction report (STR) or related information has been or will be filed, or that a money laundering, terrorist financing or proliferation financing analysis or investigation is under way, where the disclosure could prejudice that analysis or investigation.
Transaction Monitoring	The automated and manual monitoring of

End of preview

This is a preview extract. The complete document continues beyond the pages shown here.

The full document is supplied as a single, fully editable Microsoft Word (.docx) file immediately after purchase — including every remaining section, the definitions, the regulatory framework references and all appendices and templates.

Bracketed prompts such as [30 days] mark the points where your own thresholds, committee names and local regulatory references are inserted.