



ANTI-MONEY LAUNDERING, COUNTER-TERRORIST FINANCING AND COUNTER-PROLIFERATION FINANCING POLICY

Policy Owner: Group Risk Management

Policy Status: Internal Group Policy

Effective Date: 01 April 2026

Version: 1.0

1. PURPOSE

The purpose of this Policy is to establish a framework to prevent the organisation and its employees, directors, business partners, customers and other counterparties from being used for **money laundering (“ML”), terrorist financing (“TF”), proliferation financing (“PF”) or sanctions evasion.**

The organisation is committed to conducting business with integrity and complying with all applicable laws, regulations and regulatory requirements relating to anti-money laundering, counter-terrorist financing, counter-proliferation financing and sanctions.

The organisation adopts a **risk-based approach**, under which the nature and extent of due diligence and controls are proportionate to the level of risk associated with a customer, counterparty, transaction, business activity or geographic location.

Internal Use Only

This Policy is established by Group Risk Management as a Group-level internal policy to provide a consistent minimum framework for managing money laundering, terrorist financing, proliferation financing and sanctions risks across Yoma Group.

This Policy is intended for internal use within Yoma Group and does not constitute a Board-approved policy. Accordingly, formal Board approval is not required for this Policy. The Policy is maintained, reviewed and updated by Group Risk Management in accordance with the Group's internal governance framework.

Where applicable, individual entities may adopt or develop entity-level policies and procedures to meet their specific legal, regulatory and business requirements, provided that such policies and procedures are not less stringent than the minimum requirements established under this Policy.

2. SCOPE

This Policy applies to:

- all directors, officers and employees;
- contractors and consultants;
- agents and intermediaries;
- suppliers and service providers;
- customers and business counterparties, where relevant; and
- any other person acting on behalf of the organisation.

The Policy applies to relevant business relationships and transactions, including customers, suppliers, business partners, agents, distributors, investors, contractors and other third parties.

Where appropriate, joint ventures, associated companies and other business partners are encouraged to adopt equivalent AML/CTF/PF standards.

3. DEFINITIONS

3.1 Money Laundering

Money laundering is the process of disguising or concealing the illegal source, ownership or movement of money or other property obtained through unlawful activities.

Money laundering is commonly described in three stages:

Placement – introducing illegally obtained funds into the financial or legitimate economic system.

Layering – carrying out multiple transactions or arrangements to make the origin of the funds difficult to trace.

Integration – using or reinvesting the funds in the legitimate economy so that they appear to have a legitimate source.

3.2 Terrorist Financing

Terrorist financing is the provision, collection or movement of funds or other assets with the intention or knowledge that they may be used to support terrorism or terrorist activities.



Funds used for terrorist financing may originate from either legitimate or illegitimate sources.

3.3 Proliferation Financing

Proliferation financing means providing funds or financial services that are intended to support the development, production, acquisition, possession, transportation, transfer or use of weapons of mass destruction or related activities.

3.4 Beneficial Owner

The natural person who ultimately owns, controls or exercises effective control over a customer, entity, transaction or business relationship.

3.5 Politically Exposed Person

A person who is or has been entrusted with a prominent public function, together with relevant family members and close associates, as defined under applicable requirements.

4. POLICY COMMITMENT

The organisation has **zero tolerance for knowingly facilitating money laundering, terrorist financing, proliferation financing or sanctions evasion.**

The organisation shall:

1. comply with applicable AML/CTF/PF laws and regulations;
 2. identify and assess financial crime risks;
 3. conduct appropriate due diligence on customers and counterparties;
 4. identify beneficial owners and persons exercising control;
 5. conduct sanctions and relevant watchlist screening;
 6. apply enhanced due diligence to higher-risk relationships;
 7. monitor transactions and business activities for unusual or suspicious activity;
 8. promptly escalate and investigate potential financial crime concerns;
 9. report suspicious activities to the relevant authorities where required;
 10. maintain appropriate records;
 11. protect confidential information and prevent tipping-off; and
 12. provide appropriate training and awareness to employees.
-

5. RISK-BASED APPROACH

The organisation shall assess AML/CTF/PF risks based on the characteristics of its business and relationships.

Relevant risk factors may include:

Customer and Counterparty Risk

- identity and reputation;
- nature of business;
- ownership and control structure;
- beneficial ownership;
- source of funds and, where appropriate, source of wealth;
- PEP status;
- sanctions exposure;
- adverse media or negative information;
- unusual or complex business structures; and
- previous regulatory, criminal or compliance concerns.

Geographic Risk

Consideration should be given to:

- countries subject to sanctions;
- countries with higher levels of financial crime risk;
- jurisdictions with weak AML/CTF controls;
- countries associated with terrorism or terrorist financing; and
- jurisdictions associated with proliferation concerns.

Transaction and Business Activity Risk

Risk may arise from:

- unusually large or complex transactions;
- cash-intensive activities;
- international or cross-border transactions;
- transactions involving high-risk jurisdictions;
- use of multiple intermediaries;
- transactions involving unrelated third parties;
- unusual payment arrangements; and

- transactions without a clear commercial or economic rationale.

The level of controls applied shall be proportionate to the identified risk.

6. CUSTOMER AND COUNTERPARTY DUE DILIGENCE

Appropriate due diligence shall be completed before establishing a relevant business relationship or conducting a transaction where required.

For individuals, information may include:

- full name and other names;
- identification document;
- date of birth;
- nationality;
- residential and contact address;
- occupation or business activity;
- source of funds, where appropriate;
- PEP and sanctions screening; and
- other information necessary to understand the relationship.

For companies and other entities, information may include:

- legal name and registration number;
- registered and business address;
- incorporation or registration documents;
- nature of business;
- directors and authorised representatives;
- shareholders and ownership structure;
- beneficial owners;
- persons exercising effective control;
- purpose and expected nature of the relationship;
- relevant licences or registrations;
- sanctions and watchlist screening; and
- adverse media or background information.

Reliable and independent sources should be used to verify information where appropriate.

The organisation shall not knowingly establish or maintain a relationship and shall report where required by applicable law where the identity or beneficial ownership of the relevant

party cannot be satisfactorily established or where the associated risk cannot be appropriately managed.

7. ENHANCED DUE DILIGENCE

Enhanced Due Diligence (“EDD”) shall be applied where a customer, counterparty, transaction or business relationship presents higher AML/CTF/PF risk.

EDD may include:

- obtaining additional identification information;
- verifying information through independent sources;
- establishing source of funds and source of wealth;
- obtaining additional information regarding ownership and control;
- enhanced sanctions and adverse media screening;
- obtaining senior management approval;
- more frequent review of the relationship; and
- enhanced transaction monitoring.

EDD should also be applied where unusual activity or other risk indicators are identified during an existing relationship.

8. PEPs AND HIGH-RISK RELATIONSHIPS

The organisation shall identify Politically Exposed Persons (“PEPs”), relevant family members and close associates in accordance with applicable requirements.

PEP status does not automatically require rejection of a relationship. However, higher-risk PEP relationships shall be subject to appropriate enhanced controls, which may include:

- senior management approval;
- establishing source of wealth;
- establishing source of funds;
- enhanced monitoring; and
- more frequent review.

Similar enhanced measures may be applied to other high-risk customers or counterparties.

9. SANCTIONS AND PROLIFERATION FINANCING

The organisation shall maintain appropriate screening and controls to prevent dealings with persons or entities subject to applicable sanctions or targeted financial sanctions.

Screening should be conducted, as appropriate, for:

- customers and counterparties;
- beneficial owners;
- directors and shareholders;
- authorised representatives;
- suppliers and business partners;
- transaction parties; and
- other relevant persons or entities.

The organisation shall also take reasonable measures to identify and mitigate proliferation-financing risks, particularly where transactions involve:

- sanctioned persons or entities;
- high-risk jurisdictions;
- complex ownership structures;
- unusual procurement activities;
- controlled or sensitive goods;
- unusual shipping or trade routes;
- unexplained intermediaries;
- inconsistent transaction documentation; or
- attempts to conceal the ultimate beneficiary or end-user.

Where a potential sanctions or proliferation-financing concern is identified, the transaction or relationship shall be escalated and appropriate action taken in accordance with applicable law.

The organisation shall not knowingly provide funds, assets, goods or services to persons or entities subject to applicable targeted financial sanctions.

10. ONGOING MONITORING

Due diligence shall not be limited to the commencement of a relationship.

The organisation shall conduct appropriate ongoing monitoring to identify changes in risk and unusual or suspicious activities.

Monitoring should consider whether transactions and activities are consistent with:

- the customer's or counterparty's known business;
- expected transaction activity;
- stated purpose of the relationship;
- source of funds;
- ownership and control structure; and
- overall risk profile.

Where material changes or unusual activity are identified, the relationship shall be reviewed and additional due diligence may be required.

11. SUSPICIOUS TRANSACTIONS AND ACTIVITIES

Employees and relevant representatives shall promptly report any suspected ML, TF, PF, sanctions evasion or other financial crime activity to the designated Risk Management / Compliance function.

Potential warning signs may include:

- transactions inconsistent with the known business;
- unexplained large or unusual payments;
- unexplained cash transactions;
- transactions involving unrelated third parties;
- unusual movement of funds or assets;
- transactions involving high-risk jurisdictions;
- potential sanctions matches;
- false, incomplete or inconsistent documentation;
- unexplained changes in ownership;
- unnecessarily complex structures;
- attempts to avoid established controls or reporting requirements; and
- transactions with no apparent legitimate commercial purpose.

Employees are not required to prove that an offence has occurred before raising a concern.

12. REPORTING AND ESCALATION

Potentially suspicious activity shall be escalated promptly for review and investigation.

Where required by applicable law or regulation, the organisation shall submit a suspicious transaction/activity report to the relevant authority.

The organisation shall:

- assess internal alerts and concerns;
- document investigations and conclusions;
- make required regulatory reports within applicable timelines;
- maintain confidentiality; and
- take appropriate action to manage continuing risk.

Employees must not disclose information concerning a suspicious transaction report or investigation where such disclosure would constitute **tipping-off** or otherwise prejudice an investigation.

13. RECORD KEEPING

Appropriate records shall be maintained to demonstrate compliance with this Policy and applicable requirements.

Records may include:

- customer and counterparty identification;
- beneficial ownership information;
- due diligence and EDD records;
- sanctions screening results;
- risk assessments;
- transaction records;
- investigation records;
- suspicious activity reports;
- approvals and escalations;
- training records; and
- monitoring and assurance results.

Records shall be retained for the period required by applicable laws, regulations and internal policies.

14. RESPONSIBILITIES

Group Risk Management

Group Risk Management is the owner of this Policy and is responsible for:

- maintaining and updating the Policy and supporting procedures;
- establishing the Group's minimum AML/CTF/PF standards;
- providing AML/CTF/PF advice and oversight;
- coordinating Group-level AML/CTF/PF risk assessments;
- overseeing appropriate due diligence and screening requirements;
- monitoring implementation and compliance with the Policy;
- supporting investigations and escalations;
- providing training and awareness, where appropriate; and
- reporting significant AML/CTF/PF matters to senior management and the Board, where appropriate.

Management

Management is responsible for supporting the implementation of this Policy within their respective businesses and ensuring that appropriate resources and controls are in place to manage relevant AML/CTF/PF risks.

Business and Operations

Business and operational functions are responsible for:

- knowing their customers and counterparties;
- completing required due diligence;
- complying with applicable screening and approval requirements;
- identifying and escalating unusual or potentially suspicious activity;
- maintaining accurate records; and
- promptly reporting concerns to the relevant Risk Management / Compliance function.

Board of Directors

The Board of Directors retains overall oversight of material financial crime risks and may be informed of significant AML/CTF/PF matters through the established governance and reporting framework.



This Policy is approved by Group Risk Management and adopted by entity boards where required. Entity-level policies must be no less stringent.

15. TRAINING AND AWARENESS

The organisation shall provide appropriate AML/CTF/PF training to employees based on their roles and exposure to financial crime risks.

Training should cover:

- money laundering;
- terrorist financing;
- proliferation financing;
- sanctions;
- customer and counterparty due diligence;
- beneficial ownership;
- PEPs;
- suspicious activity indicators;
- escalation and reporting procedures;
- confidentiality and tipping-off; and
- employee responsibilities.

Relevant employees shall receive training upon joining and periodically thereafter, as well as when significant changes to applicable requirements occur.

16. BREACHES AND NON-COMPLIANCE

Any actual or suspected breach of this Policy shall be promptly reported to Risk Management / Compliance.

Examples include:

- failure to complete required due diligence;
- failure to perform required screening;
- deliberately bypassing AML/CTF/PF controls;
- failure to escalate suspicious activity;
- unauthorised disclosure of confidential information;
- tipping-off;

- knowingly providing false or misleading information; and
- knowingly dealing with sanctioned persons or entities.

Failure to comply with this Policy may result in disciplinary action and may expose the organisation and individuals to regulatory, civil or criminal consequences.

17. POLICY REVIEW

The Policy shall be reviewed at least annually by Group Risk Management and whenever there are significant changes to applicable laws or regulations, the Group's business activities, geographic exposure, AML/CTF/PF risks, sanctions requirements or the effectiveness of existing controls. The Policy shall be updated as necessary and maintained by Group Risk Management in accordance with the Group's internal governance framework.

18. RELATED PROCEDURES

Detailed requirements may be established through supporting procedures, including:

- Customer / Counterparty Due Diligence Procedure;
- Sanctions Screening Procedure;
- Enhanced Due Diligence Procedure;
- Suspicious Transaction / Activity Reporting Procedure;
- Third-Party Due Diligence Procedure;
- Know Your Employee Procedure; and

Where applicable, entity-level procedures may be developed to reflect the nature and risk profile of individual businesses, provided that they meet the minimum requirements of this Policy.