IGUAKO CAPITAL · Group policy

Anti-Money Laundering and Counter-Terrorist Financing

This policy sets the minimum standard that prevents the group from being used to launder the proceeds of crime or to finance terrorism. It binds all 28 jurisdictions of domicile, all 36 offices and every one of the 312 people employed by the group. It governs risk assessment, client due diligence, transaction monitoring, internal reporting and record keeping. A local requirement that sets a higher standard prevails over this text.

CODE	CATEGORY	VERSION
IGC-FC-001	Financial crime	6.1
EFFECTIVE	**REVIEW**	**OWNER**
2025-03-03	Annual, with an interim review on any change to the group perimeter	Group Head of Financial Crime

1. Purpose and scope

The group is a private financial institution with no retail business anywhere. Its money laundering exposure arises from origination in regulated life-science markets and from the movement of realised proceeds between jurisdictions. This policy makes that exposure visible, measurable and controlled at the point where capital enters the group.

The policy binds every entity in which IGUAKO Capital Holdings Ltd. holds a controlling interest, every office and representative desk, and every secondee working under a group mandate. It binds introducing intermediaries through the terms of their appointment. Where a local requirement is stricter, the stricter requirement applies without further approval.

All six divisions are in scope. Private Equity and Commercial Finance carry the largest exposure because they receive cash from operating businesses across five origination sectors. Quantitative Strategies carries the least. Controls are calibrated to that difference and are not applied uniformly for the sake of appearance.

- Sanctions screening obligations sit in IGC-FC-003 and are not restated here.
- Market abuse obligations sit in IGC-MT-001 and are not restated here.
- Retention periods are fixed by IGC-DT-003 and appear below for convenience only.

2. Definitions

Money laundering means dealing in any way with property that represents the proceeds of criminal conduct. Dealing includes possession, concealment, conversion, transfer and arranging. In most jurisdictions where the group holds a licence, suspicion alone creates an obligation, and proof of the underlying offence is not required.

Terrorist financing means providing or collecting funds with the intention that they be used for terrorism. The amount is irrelevant and the lawful origin of the funds is no defence. A transfer of US$400 receives the same treatment as a transfer of US$4 million.

A beneficial owner is any natural person who ultimately owns or controls 20 per cent or more of a client, or who controls it by other means. A politically exposed person is an individual entrusted with a prominent public function, together with immediate family members and known close associates.

3. Principles

Financial crime risk is assessed before it is managed. The group maintains a written money laundering risk assessment covering client types, products, delivery channels, sectors and geographies. Every jurisdiction added to the perimeter is scored before the first client is accepted there.

Effort follows risk. Standard due diligence applies to the majority of relationships. Enhanced due diligence applies to politically exposed persons, complex ownership chains, cash-intensive businesses and clients connected to jurisdictions scored high in the assessment. Simplified due diligence is available but is never automatic.

Suspicion is reported, not resolved on the desk. Staff are not asked to reach a conclusion about whether a crime occurred. They are asked to report the facts that trouble them, promptly, to a named person, and to keep the fact of the report confidential from the client and from the market.

4. Requirements

Requirement 4.1. No relationship is opened, and no transaction is executed, before a client file is complete and approved by two people. One approver sits outside the originating desk. Approval is recorded in the client system with a time stamp and cannot be granted retrospectively.

Requirement 4.2. Automated monitoring runs daily across client and proprietary accounts. Alerts are assigned within one business day. Level one review closes within 5 business days and level two review within 10 business days. Ageing beyond those periods reaches the Group Head of Financial Crime each week.

Requirement 4.3. Any member of staff who becomes suspicious files an internal report the same day, and in no case later than 24 hours after the concern arises. The report goes to the Group Head of Financial Crime. Discussing the report with the client is prohibited.

Requirement 4.4. Client files, monitoring output, internal reports and decisions to reject business are retained for 10 years after the relationship ends. Records are held in the group archive under a legal hold that survives the closure of any local entity.

5. Roles and responsibilities

The Group Head of Financial Crime owns this policy and the group risk assessment. The role reports to the General Counsel and Group Head of Compliance and holds a direct reporting line to the chair of the Compliance & Conduct Committee. The financial crime team numbers 19 people across five offices.

Each division head is accountable for financial crime risk inside the division. Each office has a nominated financial crime officer, appointed in writing, who is the first point of contact locally. Nominations are approved by the Group Head of Financial Crime and reviewed each year.

Internal Audit tests this policy on a cycle set by the Audit Committee. The Chief Risk Officer receives the same quarterly reporting as the Compliance & Conduct Committee. No division head may instruct a financial crime officer to withdraw or amend an internal report.

- The Group Head of Financial Crime approves every high-risk relationship before onboarding.
- Office financial crime officers hold a written appointment reviewed each year.
- Division heads confirm annually that the requirements above operated in their division.

6. Monitoring and reporting

The Compliance & Conduct Committee receives a quarterly financial crime report. It shows alert volumes, ageing, internal reports filed, external disclosures made, relationships declined and relationships exited. The Board receives the same report twice a year with commentary from the General Counsel and Group Head of Compliance.

Monitoring rules are calibrated against outcomes rather than against alert counts. A rule that produced no confirmed outcome in 12 months is reviewed and either tuned or retired, with the decision recorded. An independent review of the whole rule set is commissioned every 24 months.

7. Breaches

A breach of this policy is a disciplinary matter and may end employment. Breaches reach the Group Head of Financial Crime within 24 hours of discovery and the General Counsel and Group Head of Compliance within 72 hours. Material breaches reach the Board within 5 business days.

A breach is not closed until the root cause is documented, the control is corrected and the correction is tested. Where a breach involves a client relationship, the relationship is suspended while the review runs. Remuneration consequences are decided by the Remuneration Committee.

8. Review

This policy is reviewed annually by the Group Head of Financial Crime and approved by the Compliance & Conduct Committee. An interim review is triggered by entry into a new jurisdiction, by a change in the group perimeter, or by any confirmed control failure.

Version 6.1 took effect on 3 March 2025 and tightened the alert ageing standard from 15 business days to 10. The 2026 annual review left the standard unchanged and confirmed the next review for March 2027. Superseded versions are retained in the group archive.

Key controls

- The group money laundering risk assessment is refreshed annually and on entry to any new jurisdiction.
- No relationship opens without a completed client file approved by two people, one outside the desk.
- Automated transaction monitoring runs daily across every client and proprietary account.
- Level one alerts close within 5 business days and level two alerts within 10 business days.
- Internal suspicion reports reach the Group Head of Financial Crime within 24 hours.
- Client files, monitoring output and internal reports are retained for 10 years after exit.
- The Compliance & Conduct Committee receives a quarterly report on volumes, ageing and outcomes.
- An independent review of the monitoring rule set is commissioned every 24 months.

Related policies

- Know Your Client and Client Due Diligence (IGC-FC-002)
- Sanctions and Embargoes (IGC-FC-003)
- Financial Crime Training and Competence (IGC-FC-007)
- Whistleblowing and Speaking Up (IGC-GR-004)

Colophon