IGUAKO CAPITAL · Group policy

Fraud Prevention and Detection

Fraud against the group, against its clients and inside its portfolio companies is treated as an operational risk with a named owner and a measured control set. This policy defines internal and external fraud, fixes the payment controls that prevent it, sets the thresholds for reporting a loss and describes how an investigation runs. It covers 14 processes assessed as fraud-sensitive.

CODE	CATEGORY	VERSION
IGC-FC-005	Financial crime	2.6
EFFECTIVE	**REVIEW**	**OWNER**
2025-09-08	Annual, alongside the group fraud risk assessment	Group Head of Fraud and Operational Risk

1. Purpose and scope

The group holds US$610 million on its own balance sheet and stewards US$842 million for clients. Payment instruction fraud, invoice redirection and false accounting inside portfolio companies are the three exposures that matter most, and this policy addresses them directly rather than in general terms.

Scope covers group payments, client payments, expense claims, procurement, valuation inputs and the financial reporting of the 47 portfolio positions. It covers fraud attempted by staff, by clients, by counterparties and by outsiders impersonating any of them.

Market abuse and the misuse of inside information sit outside this policy. Cyber intrusion is governed by IGC-DT-002, although the two policies share an incident route and the same 24 hour reporting standard, so a single report satisfies both where the facts overlap.

2. Definitions

Internal fraud is dishonest conduct by a member of staff, a director or a secondee intended to produce a gain for that person or a loss to the group. External fraud is the same conduct by a person outside the group. An attempt is treated as fraud for reporting purposes.

Payment instruction fraud is an instruction to send funds to an account controlled by a fraudster, usually following a change of bank details or the impersonation of a senior officer. It is the most frequent attempt recorded against the group and the most preventable of the three main exposures.

A fraud loss is the net amount not recovered within 90 days of discovery, measured before insurance. Recovery achieved after 90 days is reported separately so that a published loss figure does not move once the quarter has closed.

3. Principles

Prevention costs less than recovery. Controls sit at the point of payment and at the point of data change, because those are the two moments at which a fraud becomes irreversible. Detective controls elsewhere in the process are useful but secondary.

No individual completes a payment alone. Segregation of duties applies to every payment path, including urgent ones. Urgency is a common feature of successful fraud and is treated as a warning sign rather than as a reason to shorten a control.

Suspicion is reported without fear of consequence. A member of staff who reports a suspected fraud in good faith is protected under IGC-GR-004, including where the suspicion later proves unfounded and where the person suspected is more senior.

4. Prevention requirements

Requirement 4.1. Any change to standing payment instructions is verified by a callback to a contact record held in the client file before the change was requested. The callback is made by a second person and logged with the time, the record used and the person spoken to.

Requirement 4.2. Payments above US$50,000 require dual authorisation. Payments above US$1 million require authorisation by a member of the Executive Committee. Authorisation limits are held in the payment system and cannot be varied by a local administrator.

Requirement 4.3. New suppliers and new client bank accounts are created by a team that cannot release payments. Creation and release are permanently separated in system entitlements, and entitlements are reviewed each quarter against the current staff list.

Requirement 4.4. Expense claims are checked against the gifts and hospitality register maintained under IGC-FC-004. Claims above US$2,500 are reviewed by the regional finance controller before payment, and claims submitted more than 60 days late are refused.

5. Detection and response

Exception reporting runs weekly and covers duplicate payments, round-sum payments, payments to newly created accounts, payments released within 30 minutes of account creation and manual journal entries above US$100,000. Every exception is cleared with a written explanation from the process owner.

A suspected fraud reaches the Group Head of Fraud and Operational Risk on the day it is suspected. Accounts are secured, entitlements are suspended and evidence is preserved before any conversation takes place with the individual concerned.

Investigations are led by the fraud team with the General Counsel and Group Head of Compliance. Where a member of staff is implicated, the Chief Operating Officer is informed and the individual is suspended on full pay while the investigation runs.

6. Roles and responsibilities

The Group Head of Fraud and Operational Risk owns this policy, the fraud risk assessment and the exception reporting suite. The role reports to the Chief Risk Officer and presents to the Risk & Valuation Committee each quarter with loss and attempt data.

Regional finance controllers operate the payment controls in their region. Division heads own fraud risk inside the portfolio companies they oversee and confirm each year that every controlled company operates segregation of duties on payments.

- Losses above US$25,000 reach the Chief Risk Officer within 24 hours.
- Losses above US$250,000 reach the Board within 5 business days.
- Attempted frauds are reported whether or not a loss followed.

7. Reporting, breaches and review

The quarterly report to the Risk & Valuation Committee shows attempts, losses, recoveries, control failures and remediation status by region. The annual fraud risk assessment scores 14 processes and is approved by the Chief Risk Officer before the budget round.

Overriding a payment control is a breach whether or not a loss follows. Overrides are logged automatically and reviewed weekly. A second override by the same person in a rolling 12 month period is referred to the Chief Operating Officer for a conduct decision.

This policy is reviewed annually. Version 2.6 took effect on 8 September 2025 and added the callback requirement for changes to standing instructions. Investigation files, exception reports and override logs are retained for 10 years.

Key controls

- Changes to standing payment instructions are verified by a logged callback made by a second person.
- Payments above US$50,000 require dual authorisation and above US$1 million an Executive Committee approver.
- Account creation and payment release are permanently separated in system entitlements.
- System entitlements are reviewed each quarter against the current staff list.
- Weekly exception reporting covers duplicates, round sums, new accounts and large manual journals.
- Losses above US$25,000 reach the Chief Risk Officer within 24 hours of discovery.
- The fraud risk assessment scores 14 processes and is approved annually by the Chief Risk Officer.
- Investigation files and override logs are retained for 10 years.

Related policies

- Information Security (IGC-DT-002)
- Whistleblowing and Speaking Up (IGC-GR-004)
- Anti-Money Laundering and Counter-Terrorist Financing (IGC-FC-001)
- Operational Resilience (IGC-GR-003)