NIBC
FRAUD PREVENTION POLICY SUMMARY

November 2021

NIBC

1. SUMMARY OF POLICY

NIBC's Fraud Prevention policy summarises the various controls designed to prevent, detect and investigate any suspicions of fraud, including illegal tax evasion, within NIBC, and ensure compliance with all relevant legal and regulatory requirements in these areas.

1.1 Core principles and guidance

No acceptance of Fraud

NIBC does not want or accept any involvement in fraud. Managers and employees are obliged to report actual or suspected fraud or misconduct to Compliance, who will determine appropriate follow-up action.

If suspicions of internal fraud are established, action will be taken against violators.

How to fight Fraud

NIBC actively fights fraud under its Fraud Prevention Policy, in which its framework for prevention, detection, deterrence and investigation is explained.

1.2 Definitions

Fraud is generally described as "any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and / or the perpetrator achieving a gain".

Internal fraud is best described as employees (including contractors) who intentionally deceive others to achieve an advantage, benefit or gain.

External fraud is best described as clients, business partners or other third parties who are deceiving NIBC employees to achieve a gain.

2. NIBC FRAUD PREVENTION FRAMEWORK

2.1 Key defences against Fraud and principal roles & responsibilities

- All employees (awareness, prevention, detection, escalation of fraud).
- Compliance (policy implementation, training, monitoring effectiveness)
- Management (promote culture of awareness and prevention).

2.2 Key High-level controls and responsibilities

Prevention of Fraud in most organisations depends upon:

- A culture of honesty and ethics;
- Effective risk assessment;
- Active Internal Control; and
- Awareness raising and training

2.3 Measures and Defences to combat Fraud

An effective fraud prevention) strategy should be recognised as having four main elements:

- Prevention;
- Detection;
- Deterrence; and

- Response.

Prevention, detection and deterrence of fraud comprise the key elements to an effective fraud prevention framework. NIBC applies all these controls within its organisation and activities. We place particular focus on prevention and deterrence as the most effective up-front controls, as we do not wish fraud to arise within our business.

The responsibility for the prevention, detection and deterrence of fraud lies with every individual employee.

Employees must be aware of the types of misconduct, impropriety and criminal behaviour that might occur within their area of responsibility and be alert for any signs of irregularity. Responsibilities in this regard will increase in accordance with employee seniority, role and scope of activities.

Managers and employees are legally obliged to report actual, attempted or suspected incidences of fraud.

Any employee who discovers or suspects a fraud, misappropriation or other serious irregularity is required to report this internally without delay.

2.3.1 Risk Assessment (prevention) principles

Responsible senior management within each business unit should ensure NIBC's established risk assessment processes and planning address the most relevant material factors, drivers and likely causes of internal and external fraud. These should be reviewed and updated on at least an annual basis, in particular, with due care and attention given to specific fraud risks and trends that may arise within the scope and activities of business.

Where a business line, activity, sector or jurisdiction identifies a material and relevant risk of fraud, corresponding risk mitigation measures should be implemented proportionate to the risk factor(s) identified.

Evidence such as regular monitoring reviews and management reporting should be maintained to ensure that the persons responsible for fraud risk mitigation controls and actions have taken reasonable steps to monitor their effectiveness.

2.3.2 Internal controls (prevention and detection)

Line management is responsible for the design, implementation and reinforcement of effective controls to address relevant material fraud risks where identified.

The following are the general principles of a successful internal fraud prevention strategy:

- System access: requirements and restrictions to sufficiently guarantee that only authorized personnel can access the relevant applications.
- Segregation of duties: duties are divided so no one person has sole control over a key function or activity;
- Authorisation and approval: Proposed transactions are authorized when they are consistent with policies and funds are available;
- Custodial and security: Responsibility for custody of assets is separated from related record keeping;
- Record-keeping; Comprehensive and accurate records of activities provide an essential audit trail.
- Review and reconciliation: Records are examined and reconciled to determine that transactions were properly processed and approved;
- Physical controls: Equipment, inventories, cash, and other assets are secured physically, counted periodically, and compared with amounts shown on control records;
- Documentation: Well-documented procedures and practices promote employee understanding of duties and help ensure continuity during employee absences or turnover.

2.3.3 Training and Awareness

Well-trained and supervised employees help ensure that control processes function properly, increasing

awareness of fraud risks and reinforcing a culture of intolerance to fraud generally. NIBC's Compliance department provides mandatory Fraud training to all employees annually.

Fraud prevention training should address the following topics as relevant to the business area or unit:

- Significant fraud risks relevant to the business area or unit;
- NIBC preventative and ethical culture (e.g. NIBC Code of Conduct);
- Key controls in place to prevent fraud and testing of the effectiveness of such controls ;
- 'Red flags' (fraud indicators) to look out for;
- Steps to take where suspicions of fraud arise; and
- Contact points for reporting or whistleblowing suspicions of fraud.

3. REPORTING AND RECORD-KEEPING

3.1 Reporting Suspicions of Fraud

Managers and employees have a duty to report actual, attempted or suspected incidences of fraud. Any employee who discovers or suspects that fraud may be occurring should escalate this to his or her line manager.

Any incidence of fraud (actual, attempted or suspected) concerning information security and/or data protection will be reported separately under the relevant requirements maintained by NIBC's Corporate Information Security Officer (CISO) and Data Protection Office (DPO).

Senior and line management, working with Compliance, should ensure that all employees are sufficiently aware of fraud reporting and escalation and confident in using them where necessary.

3.2 Whistle Blowing

Employees are reminded that, notwithstanding the above arrangements and requirements, they have the right to report any concerns of illegal behaviour or serious misconduct within NIBC anonymously to a Trusted Representative under the NIBC Whistle Blowing Policy.

It is NIBC's policy that no employee will be sanctioned for making a report in good faith, even if this results in the loss of business or some other detriment.

3.3 Record-keeping and retention of documents

All business and support units within NIBC should maintain detailed and accurate financial records and have appropriate internal controls in place to act as evidence for all receipts and payments.

Where suspicions of fraud are escalated and reported within NIBC, any records and documentation pertaining to the matters reported must be retained securely and in strict confidence, as these may be subject to external investigation, including by law enforcement and / or regulatory agencies.

4. Monitoring

NIBC's Compliance department monitors the effectiveness of this Policy. Compliance will report any findings of non-compliance with its requirements to the employee(s) responsible and to senior management. The risks of internal and external fraud are included amongst those identified, assessed responded to, monitored and reported according to NIBC's Risk Management Framework.

Reporting includes (not necessarily limited to):

a) NIBC's annual bank-wide Systemic Integrity Risk Analysis (" SIRA ") review process, which addresses all material integrity risks to the Bank's business activities and operations; and
b) (for UK Branch) the Money Laundering Reporting Officer (" MLRO ")'s Annual Report to Managing Board, produced as at calendar year end.

Any need for improvements and/or remedial measures will be applied as soon as possible. Employees are encouraged to offer their feedback on this policy if they have any suggestions for how it may be improved. Feedback of this nature should be addressed to the Compliance department.