FRAUD PREVENTION POLICY

November 29, 2023

TABLE OF CONTENTS

1. INTRODUCTION 2
   - 1.1 General 2
   - 1.2 Definitions 2
   - 1.3 Applicability 2
   - 1.4 Purpose 2
   - 1.5 Effective Date 2
   - 1.6 Ownership 3
   - 1.7 Internal policies, standards and/or procedures relating to Fraud Prevention Policy 3

2. NIBC FRAUD PREVENTION POLICY 3
   - 2.1 Purpose and scope of fraud prevention policy 3
   - 2.2 Within Fraud Prevention Policy Core principles and guidance 3

3. NIBC FRAUD PREVENTION FRAMEWORK 4
   - 3.1 Key principles and requirements 4
   - 3.2 Key defenses against Fraud and principal roles & responsibilities 4
   - 3.3 Key High-level controls and responsibilities 4
   - 3.4 Measures and Defenses to combat Fraud 4
     - *3.4.1 Risk Assessment (prevention) principles 4*
     - *3.4.2 Internal controls (prevention and detection) 5*
     - *3.4.3 Training and Awareness (fraud prevention, detection, and deterrence) 5*
     - *3.4.4 Reporting and escalation (fraud prevention, detection, and response) 5*
   - 3.5 Reporting of fraud 5
   - 3.6 Whistleblowing 6
   - 3.7 Record-keeping and retention of documents 6

4. POLICY EXCEPTIONS, MONITORING COMPLIANCE AND SANCTIONS 6
   - 4.1 Policy Exceptions 6
   - 4.2 Monitoring 7
   - 4.3 Sanctions 7

1. INTRODUCTION

1.1 General

The policy summarizes 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.

1.2 Definitions

Employees All employees of NIBC (including the international offices) and all independent contractors and/or temporary staff of NIBC working under the management and/or supervision of NIBC.

NIBC NIBC Holding N.V. and its subsidiaries (including, amongst others, NIBC Bank N.V.) and their international offices, as well as all domestic and foreign legal entities in which NIBC Holding N.V. has a direct or indirect (equity or voting) interest of more than 50%. Within this definition the (consolidated) equity interests in companies acquired and/or held as a participation/investment, which are not financial institutions, are excluded. Beequip B.V. and Fin Quest B.V. (and if applicable their respective subsidiaries) are however considered not in scope of this Policy. The applicability of this Policy to any new entities acquired by NIBC Holding N.V. or by any of its group companies must be assessed and decided upon on a case by case basis and this definition will be amended accordingly, if needed, at the latest at the next yearly update of this Policy. Companies which would otherwise fall within this definition but which have agreed exceptions/individualised policies applicable to the subject matter covered by this policy (and which has been notified to the Policy Officer of NIBC Bank N.V.) are excluded.

Fraud Fraud is best 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 risk is best described as the risk that a person acts dishonestly against NIBC or our customers for advantage or gain (this may involve a collusion between staff and a noncustomer).

External fraud risk is best described as the risk that a person acts dishonestly against NIBC or our customers for advantage or gain.

1.3 Applicability

The policy applies to all business and activities carried out by NIBC or on behalf of NIBC by its associated persons, which includes NIBC's subsidiaries and employees as defined in Section 1.2 above. NIBC will take steps to prevent any occurrence of fraud, wherever it identifies a responsible interest in doing so.

1.4 Purpose

The policy aims to detect, act, keep record and report in a timely manner when a fraud case occurs, prevent fraudulent activity within, by and / or on behalf of NIBC, apply a zero-tolerance approach as regards to internal fraud, and keep the external fraud risk within NIBC's risk appetite, which is LOW.

1.5 Effective Date

This Policy came into force on December 8, 2020, and supersedes the relevant sections of the previous Global Anti-Fraud, Bribery and Corruption Policy. NIBC reserves the right to amend this Policy from time to time if circumstances (e.g., changes to legislation and regulations) make this

necessary. Any material changes to this Policy will be approved by the RMC and will be notified to the relevant stakeholders, such as employees, as appropriate.

1.6 Ownership

Compliance within NIBC is the designated owner of this Policy and, as such, responsible for the maintenance and review of the document every 2 years, or more frequently if circumstances (such as changes in relevant laws or regulations) so require.

1.7 Internal policies, standards and/or procedures relating to Fraud Prevention Policy

- AO/IC Policy
- Code of Conduct
- Whistle Blowing Policy
- Special Investigation Policy
- Incidents Policy
- Engagement Committee Policy
- Corporate Information Security Policy
- Risk Management Framework
- Compliance Framework
- Sustainability Framework

2. NIBC FRAUD PREVENTION POLICY

2.1 Purpose and scope of fraud prevention policy

The purpose of this l Fraud Prevention Policy is to set out the steps to be taken in order to achieve the following:

1. **prevent** or minimise the risk of fraud,
2. **detect** incidences / indications of fraud and
3. create a hostile **(deterrent)** environment to fraud within our business.

Prevention, detection, and deterrence of fraud comprise the key elements to an effective fraud prevention framework. NIBC applies all these measures 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.

2.2 Within Fraud Prevention Policy Core principles and guidance

Please read this policy (NIBC's Fraud Prevention Policy) in full. This includes the fraud prevention framework that NIBC applies in prevention, detection, and deterrence of fraud. Ensure you follow the measures that help prevent and combat fraud, including segregation of duties and maintaining records of business activities, particularly involving clients, counterparties, contractors, employees, and key stakeholders.

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 a fraud, misappropriation or other serious irregularity is required to report this to his line manager and register in [system]. Alternative escalation is through the process according to Whistleblowing Policy. Attempted or suspected incidences of fraud is to be reported to the Head of Compliance immediately . Should a case reported to the Head of Compliance judged as an actual fraud case, the case must be registered in [system].

Any unreasonable delay, omission, or failure to report, or obstruction of any escalation or investigation (where fraud is known or suspected to have occurred) may be assumed to be in breach of this policy.

Definitions of fraud are increasingly wide-ranging. Included in this is tax evasion, which is the subject of a separate Tax Position Statement. Involvement in fraud is a serious criminal offence. Should you become suspicious please report without delay.

3. NIBC FRAUD PREVENTION FRAMEWORK

3.1 Key principles and requirements

NIBC's stance on Fraud
NIBC does not want or accept any involvement in fraud. Managers and employees are obliged to report actual fraud via [system], and suspected fraud to the Head of 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 (a) the Three Lines of Defence principle as described in its Risk Management Framework and (b) its Fraud Prevention Policy, in which its strategy for prevention, detection, deterrence and investigation is explained.

3.2 Key defenses against Fraud and principal roles & responsibilities

- All employees (awareness, prevention, detection, escalation of fraud, segregation of duties, access & ID management, 4 eyes check principle, etc.).
- Compliance (policy implementation, training, monitoring effectiveness)
- Soft-control (promote culture of awareness and prevention).

3.3 Key High-level controls and responsibilities

- Prevention of Fraud in most organisations depends upon:
- A culture of honesty and ethics;
- Effective fraud prevention framework; and
- Awareness raising and training

3.4 Measures and Defenses to combat Fraud

- An effective fraud prevention strategy should be recognised as having four main elements:
- Prevention;
- Detection;
- Deterrence; and
- Response.

3.4.1 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 via the SIRA and RCSA processes, 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 (controls and actions) 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. This includes Key Risk Control Effectiveness testing as required per ORM Policy/Procedures.

3.4.2 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;
- 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.

3.4.3 Training and Awareness (fraud prevention, detection, and deterrence)

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.

Fraud prevention training is undertaken wherever practicable on the following basis:

- As part of induction training and regularly thereafter:
- Covering all employees;
- Provided partly or fully on an in-house basis; and
- Ensuring follow-up and response to queries.

Fraud prevention training addresses 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.., 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.

3.4.4 Reporting and escalation (fraud prevention, detection, and response)

Senior and line management, working with Compliance, should ensure that all employees are sufficiently aware of fraud reporting obligation and escalation processes (as set out in Section 3.6 this Policy) and confident in using them where necessary.

3.5 Reporting of fraud

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

On receiving notification of a suspicion that fraud may be occurring / have occurred, Line management should inform the Head of Compliance (or in his absence a member of the Compliance Team) and seek advice on further action, as appropriate to the seriousness and sensitivity of the matters identified. Compliance will determine what additional measures are necessary in accordance with the potential seriousness and likely impact of the alleged offences. This should include where necessary alerting the appropriate law enforcement and /or regulatory authorities.

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

Line management should also record any known incidence of fraud as an Operational Risk Event, if necessary, in consultation with ORM. In case of suspicious fraud cases the Head of Compliance shall be informed. Similarly, where deemed applicable, the requirements of the Incidents and/or Special Investigations Policies should also be observed. Where an employee makes a good faith disclosure to a Confidential advisors under the Whistleblowing Policy, the confidentiality requirements of that Policy should be treated as paramount.

3.6 Whistleblowing

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 Confidential Advisors under the Whistleblowing Policy. The Confidential Advisors shall not be required to disclose such matters in accordance with Section 3.6 of this Policy (see above). This applies in specific circumstances where employees have personal reservations that they may be treated unfairly despite disclosing such matters in good faith.

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.

3.7 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. Transactions or disbursements that appear unusual and/or suspicious, not properly authorised, or approved and / or have no obvious rationale or explanation should be considered as potential 'red flags' and reported to the line manager, thereafter to the Head of Compliance, for further query and investigation.

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. It is generally deemed to be a serious offence intentionally to destroy, delete, dispose of, alter, or tamper with any such records or documents, or make any attempt to do so, and accordingly, access should be restricted to a 'need to know' basis.

4. POLICY EXCEPTIONS, MONITORING COMPLIANCE AND SANCTIONS

4.1 Policy Exceptions

Due to the potential legal and reputational consequences of fraud, it is not anticipated that exceptions to this Policy will arise or be requested.

4.2 Monitoring

NIBC Compliance 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 Systematic 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 Compliance.

4.3 Sanctions

Because of the seriousness of the potential consequences of fraudulent activity, breach of NIBC's Fraud Prevention Policy in this context is a disciplinary matter with sanctions up to and including dismissal.

NIBC does not want or accept any involvement in fraud. This means that proportionate actions will be taken against anyone within our organisation who perpetrates or encourages such behaviours, whether wilfully, knowingly, recklessly, or through a position of influence.

Any employee found to have violated this Policy may be subject to disciplinary action, depending on the materiality and frequency of the breach. Criminal breaches of the law on fraud are likely to result in prosecution and serious legal penalties against offenders.