



HAITONG

REGULATION No. COM23.R65
Fraud Prevention Regulation of Haitong Bank, S.A.

Approved by the Board of Directors
on 25/06/2026

TABLE OF CONTENTS

1. OBJECTIVE.....	3
2. LEGAL FRAMEWORK	3
3. RECIPIENTS	4
4. RESPONSIBILITY	4
5. FRAUD	4
5.1 DEFINITION AND GOVERNANCE	4
5.2 TYPES OF FRAUD AND CONTROLS	5
5.2.1 CONFLICTS OF INTEREST	5
5.2.2 AML-CFT.....	6
5.2.3 BRIBERY & CORRUPTION.....	7
5.2.4 PAYROLL	8
5.2.5 REIMBURSEMENTS	9
5.2.6 DISBURSEMENTS	11
5.2.7 FINANCIAL STATEMENTS	12
5.2.8 NON-FINANCIAL STATEMENTS.....	13
5.2.9 CYBERSECURITY	14
5.3 OTHER INTERNAL RULES.....	15
5.4 DETECTION, ANALYSES AND RESOLUTION	18
5.4.1 INTERNAL REPORT	18
5.4.2 EXTERNAL REPORT	19
5.5 MONITORING AND EVALUATION	19
5.5.1 RISK ASSESSMENT.....	19
5.5.2 LIMITATIONS OF INTERNAL CONTROLS	19
5.5.3 EVALUATION AND EFFECTIVENESS OF CONTROLS.....	20
6. ARCHIVE	20
7. DISCLOSURE	20
8. CONTROL OF VERSIONS	21
9. ANNEXES.....	22
9.1. ANNEX 1 – FRAUD PREVENTION RESPONSIBILITY MATRIX.....	22

1. OBJECTIVE

This Regulation establishes the general principles, responsibilities, and rules for fraud prevention at Haitong Bank, S.A. (hereinafter referred to as "Haitong Bank" or the "Bank").

To comply with legal and regulatory obligations, the Bank implements robust measures designed to minimize the risk of fraud across its operations and activities.

Accordingly, fraud risks are internally identified, and the correspondent internal controls are implemented as to prevent, detect and respond to fraud events.

This Regulation aims to serve as a guide, capturing the various controls implemented that are designed to prevent, detect, and investigate any suspicions of fraud and ensure compliance with all relevant legal and regulatory requirements.

While the Bank's Board of Directors holds ultimate responsibility for preventing and detecting fraud within the Bank, the daily oversight of anti-fraud efforts lays in all the Bank's employees.

2. LEGAL FRAMEWORK

This Regulation is subject to the following laws, regulations and other guidelines:

- Decree Law No. 109-E/2021 ("General Regime of Prevention of Corruption").
- Law No. 83/2017 of 18 August (Portuguese AML/CFT framework).
- Law No. 93/2021 (General Whistleblower Protection Framework).
- Decree-Law No. 48/95 of 15 March (Portuguese criminal code)
- Convention on Bribery of Foreign Public Officials in international business transactions from the Organisation for Economic Cooperation and Development ("OECD").
- 1997 European Union Convention against Corruption involving Officials (EU Convention against Corruption).
- 2003 Council Framework Decision on Combating Corruption in the Private Sector.
- Criminal Law Convention on Corruption of the Council of Europe.
- United Nations Convention against Corruption.
- UK Bribery Act.
- ISO 37001, an international standard that provides requirements and guidance for establishing and implementing an anti-bribery management system.
- Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law.
- Regulation (EU) No 596/2014 – Market Abuse Regulation.

3. RECIPIENTS

- a. The content of this Regulation represents a minimum standard that shall apply to the Bank, its subsidiaries, branches and representative office (“Haitong Bank Group”), with the necessary adjustments in light of the specific operations and activities effectively carried out.
- b. In case of conflict between any provision of this Regulation and the local laws and regulations applicable to any of the Bank’s subsidiaries, branches or representative office, the relevant local laws and regulations shall prevail.

4. RESPONSIBILITY

- a. This Regulation is sponsored by the Compliance Department.
- b. This Regulation should be reviewed by the Compliance Department every two years, or whenever necessary.

5. FRAUD

5.1 DEFINITION AND GOVERNANCE

Fraud can be broadly defined as an intentional act of deceit to obtain an unjust/illegal advantage perpetrated by a fraudster with the aim of deceiving or harming a person or an organization, for his or her own or a third party’s benefit, to avoid a certain obligation or to cause losses for a certain organization.

Fraud can be differentiated between internal fraud and external fraud.

Internal fraud, also known as insider fraud, is carried out from inside an organization by its own employees. On the other hand, external fraud refers to fraudulent behavior perpetrated by individuals outside the organization.

The Board of Directors have a primary responsibility in the oversight of fraud prevention in the Bank, by setting the “tone at the top” and ensuring institutional support for ethical and responsible business practices at the highest levels.

A strong ethical culture is one of the most important anti-fraud mechanisms an organization can have because it influences how employees respond to every organizational process or transaction.

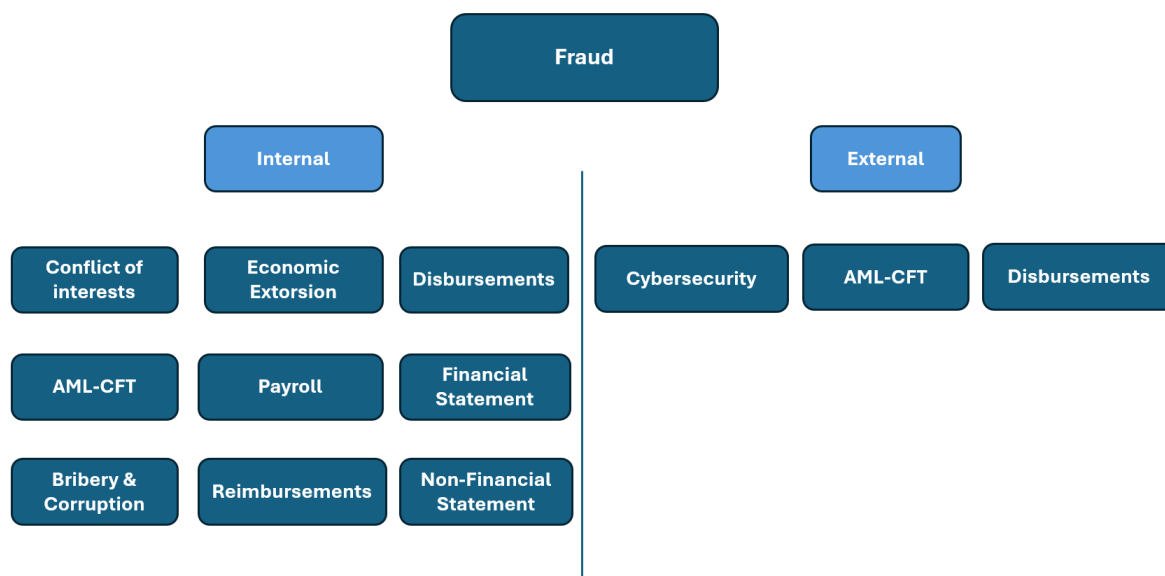
In addition, internal and external auditors play a key supporting role in the Bank’s fraud risk management framework, through independent assessments and audit activities that help ensuring that anti-fraud controls are properly designed, implemented, and operating effectively. Auditors provide assurance to both the Board of Directors on the adequacy of the Bank’s internal control environment and contribute to the continuous improvement of fraud prevention efforts.

All employees must understand they share responsibility for preventing, detecting, and reporting instances of fraud. Fraud prevention is a collective effort. Every staff member is accountable for helping to deter and defend the Bank from fraud. While all employees are committed to combating fraud, specific anti-fraud control duties are assigned to certain managers and employees based on the nature of their role or as stipulated by the Bank's internal rules.

Fraud prevention requires a coordinated effort across all levels of the Bank. While leadership defines and drives the strategy, its success depends on ongoing commitment, vigilance, and accountability from all stakeholders.

5.2 TYPES OF FRAUD AND CONTROLS

While instances of fraud may take various forms, the chart below provides an overview of the types of fraud the Bank perceives as more material based upon its current activities and operations:



The following sections will have for each type of fraud a general description of how the same can materialize, the relevant controls in place, and the respective owners.

INTERNAL

5.2.1 Conflicts of interest

a) Description

A conflict of interest represents a situation whereby an entity or individual have conflicting interests and the serving of one interest may involve the detriment of another.

While not inherently fraudulent, conflicts of interest can create fertile ground for fraudulent behavior when left unmanaged or deliberately concealed.

b) Controls

This matter is addressed under COM02R02 - Conflicts of Interest Prevention and Management Regulation, COM12.PM.030 Prevention and Management of Conflicts of Interest Procedure and Procedure No. COM17.PM042, Restrictions and Personal Transactions. These internal rules play a crucial role in preventing fraud by ensuring that the Bank can identify, prevent, and manage situations where personal or external interests could compromise professional responsibilities.

c) Ownership

The primary ownership for identifying, managing, and preventing conflicts of interest lies with each and every employee of the Bank, as they must ensure that their conduct is carried out with objectivity, independence, and in alignment with the Bank's ethical and regulatory standards.

Additional ownership is also provided by the following stakeholders:

- Compliance on the identification of potential conflicts of interest in transactions.
- Corporate secretaries of the Bank's corporate bodies and committees.

5.2.2 AML-CFT

a) Description

Anti-Money Laundering and Countering the Financing of Terrorist ("AML-CFT") refers to the set of controls designed to detect, prevent, and report activities that involve the laundering of illicit funds or the use of financial systems to finance terrorism.

b) Controls

The Bank's AML-CFT risk model is addressed under COM08.R09 Anti-Money Laundering and Countering the Financing of Terrorist Regulation and over a mix of procedures, IT systems and trainings, designed to comply with its lawful obligations given the specificities of the Bank's business activities over its relevant dimensions.

The AML-CFT Regulation is a critical component of the Bank's overall strategy to prevent fraud and financial crime. By establishing robust procedures for KYC, customer due diligence, transaction monitoring, and suspicious activity reporting, the regulation helps detect and deter fraudulent schemes that often involve illicit funds or concealment of criminal proceeds. It ensures that the Bank is not misused as a channel for illegal activities, reinforcing the integrity of the financial system.

c) Ownership

The primary ownership for preventing money laundering and the financing of terrorism (AML-CFT) lies with the Front Office areas of the Bank. Each business unit is expected to apply appropriate due diligence, report suspicious activity, and follow internal procedures and regulatory requirements to ensure the integrity of the Bank's operations. These areas constitute the first line of defense, and as such, are directly accountable for the proper implementation of AML-CFT controls in their day-to-day activities.

Additional ownership is also provided by the following:

- Operations Department within the onboarding and regular follow-up of the clients / counterparties activities.
- Compliance Department by providing guidance, monitoring, and oversight across the Bank, ensuring the implementation of policies, supporting training initiatives, performing risk assessments, and reporting to regulatory authorities when necessary.
- Auditors (Internal and External) via their regular assessment on the adequacy and effectiveness of the Bank's AML-CFT framework.

5.2.3 Bribery & Corruption

a) Description

Bribery & corruption are forms of fraudulent misconduct that involve the abuse of power for personal or corporate gain, often through the offering or acceptance of improper advantages. Such practices not only

violate legal and ethical standards but also expose the Bank to significant reputational and regulatory risks.

b) Controls

Bribery & Corruption is addressed under COM07R08 Anti-Bribery and Corruption Regulation. This Regulation is a vital instrument in the Bank's efforts to prevent fraud and promote a culture of integrity. By clearly prohibiting all forms of bribery and improper influence, both within the Bank and in its external relationships, the regulation helps eliminate opportunities for corrupt practices that could lead to financial and reputational harm. It sets strict standards of conduct, promotes transparency in decision-making, and reinforces accountability among employees and third parties.

The Bank's processes and controls to mitigate, prevent and manage Bribery & Corruption risks include:

- i) Plan for the prevention of risks of corruption and related infractions.
- ii) Provide anti-bribery training to employees.
- iii) Control benefits provided to individuals and third parties- such as hospitality, gifts, and donations – to ensure they do not serve a corrupt purpose.
- iv) Implemented a Whistleblowing Regulation in respect of the receipt and processing of reports of wrongdoings by employees or third parties to investigate and address any suspected or actual bribery.

c) Ownership

The primary ownership for the prevention of Bribery & Corruption lies with each employee of the Bank.

Additional ownership is also provided by the Compliance Department, which has developed and implemented a dedicated Anti-Bribery and Corruption Program aligned with legal and regulatory requirements.

5.2.4 Payroll

a) Description

Payroll refers to the process of managing employee compensation, including salaries, bonuses, deductions, benefits, and related tax and social security obligations. It involves accurate and timely calculation and distribution of payments to employees based on their employment terms, attendance, and performance.

Due to the high volume of financial transactions, sensitive personal data involved, and the potential for internal manipulation, payroll is a critical area of focus in any fraud prevention strategy. Common types of payroll fraud include the creation of fictitious or “ghost” employees, unauthorized changes to salary information, inflated overtime or bonus payments, duplicate payments, and falsified working hours.

b) Controls

This matter is addressed under Procedure No. HRD06.PM135 Payroll Management. This document outlines the payroll processing procedures and covers the entire process, starting from the creation of employee records and ending with the calculation of social contributions and taxes, as well as the collection of relevant data, payment of salaries, and associated bookkeeping tasks.

The Bank's payment of salaries is a transparent process. To achieve this, the Bank has implemented the Staff Costs Management procedure, identifying all staff-related costs and outlining how each category of cost is processed and approved. The Staff Costs Management Procedure describes the processes related with the processing and approval of different types of staff costs. The sources of staff costs mainly arrives from the Bank's annual budget or in a case-by-case basis. The Bank's annual budget is approved by the Board of Directors on a yearly basis. For case-by-case staff costs, there are different approval authorities, depending on the nature of the cost and the amount.

Salary processing and payroll management is executed fully in line with the aforementioned procedure.

c) Ownership

The primary ownership for the accurate and secure management of Payroll lies with the Human Resources Department, who is accountable for maintaining up-to-date employee records, validating employment status, processing salary and ensuring that all payroll transactions are legitimate, authorized, and aligned with internal rules and legal obligations.

Additional ownership is also provided by the Finance Department, which collaborates with the Human Resources Department to prevent and detect potential fraud or errors in the payroll process.

5.2.5 Reimbursements

a) Description

Reimbursements refer to the process through which employees and other stakeholders are repaid for eligible expenses incurred on behalf of the Bank, including but not limited to travel, accommodation, representation, and operational disbursements.

While reimbursements are a legitimate part of business operations, they are also considered a potential area of fraud risk, particularly in cases where:

- False or inflated expense claims are submitted;
- Personal expenses are misrepresented as business-related;
- Supporting documentation (e.g., invoices or receipts) is falsified or manipulated;
- Approval processes are bypassed, or collusion occurs between employees and approvers.

b) Controls

This matter is addressed under Procedure No. FIN29.PM362 CAPEX and OPEX Management. The Bank has implemented specific processes and controls for the approval and validation of reimbursements through this Procedure, particularly concerning representation expenses.

Employee reimbursement requests are initiated through intranet forms and processed across multiple departments. The Legal Department – Information and Documentation Section is responsible for scanning and registering all documents in the Workflow system, ensuring proper traceability. Expenses are then reviewed and approved electronically according to the applicable rules and predefined approval thresholds. The Finance Department verifies the completeness and accuracy of the supporting documentation, records the transactions in SAP, and ensures compliance with internal procedures. Once approved, the Operations Department executes the payments and manages all logistics related to cash advances.

Additional control mechanisms include defined time limits for submitting reimbursement requests after the expense has been incurred, as well as clearly established documentation requirements to ensure compliance with relevant regulations, including tax rules. All documents are routed through the Workflow system for validation and auditability. Monitoring procedures are in place to identify non-compliant or overdue reimbursements, which may be settled through payroll deductions in coordination with HR.

These requirements ensure a controlled, auditable, and standardized process, reducing the risk of fraudulent or unauthorized reimbursements and reinforcing the Bank's internal control environment.

c) Ownership

The Finance Department holds primary responsibility for the control and oversight of the reimbursement process. This function is supported by:

- Line Managers and Heads of Department, who validate and approve reimbursement requests submitted by their teams;
- Legal Department – Information and Documentation Section, which ensures proper registration and traceability of documentation in the Workflow system;
- Operations Department, which executes the approved payments and manages cash advances logistics.

Approval of reimbursements follow a structured multi-level authorization framework, with thresholds defined according to the nature and amount of the expense.

5.2.6 Disbursements

a) Description

Disbursements refer to the outflow of funds from the Bank to third parties, including acquisitions, payments to suppliers, service providers, regulators, tax authorities, and other operational or strategic expenses. Due to the financial impact and volume of these transactions, disbursements are considered a key area of fraud risk exposure.

Subsequently, such payments should be conducted prudently and through an organized process, raising the stakeholders' consciousness and awareness concerning all contracts and services requests under their responsibility.

b) Controls

Procedure No. FIN29.PM362 CAPEX and OPEX Management incorporates robust control mechanisms throughout the procurement and payment cycle.

Multiple departments are involved to ensure proper segregation of duties and process integrity. The Legal Department – Information and Documentation Section is responsible for receiving, scanning, and registering invoices in the Workflow system, while the relevant business areas confirm that the goods or services were delivered as agreed and approve the invoices within their delegated authority levels. The Finance Department reviews the supporting documentation, records the transactions in SAP, and authorizes payments in accordance with the established approval thresholds. The Operations Department then executes the payments and oversees supplier registration as well as the validation of bank account details.

In addition, all payments are governed by predefined approval levels, ensuring that each approver can only authorize expenses within their assigned financial limits. Reporting also forms an integral part of the control environment. Finance Department prepares monthly and semi-annual reports, which are shared with the Executive Committee and provide detailed analysis by supplier and cost category.

These processes are designed to reduce the risk of unauthorized, excessive, or fraudulent payments, while promoting accountability and alignment with internal rules and legal obligations.

c) Ownership

The Finance Department holds primary responsibility for the oversight and execution of disbursements. This ownership is exercised in coordination with:

- Legal Department – Information and Documentation Section, which ensures proper registration and traceability of invoices in the Workflow system;
- Business Units and Executive Committee Members, who validate and approve expenses according to predefined thresholds;
- Operations Department, which executes payments and manages supplier registration and bank account verification.

Disbursements are subject to a multi-level approval framework, ensuring that no single individual controls the full payment cycle. This structure reinforces transparency, accountability, and fraud prevention.

5.2.7 Financial Statements

a) Description

Financial statements are formal records that reflect the Bank's financial position, performance, and cash flows over a specific period. These include, the balance sheet, income statement, statement of cash flows, and statement of changes in equity, among others. They are essential for internal and external stakeholders, including regulators, investors, and auditors, and form the basis for strategic and operational decision-making.

Fraudulent manipulation of financial information—whether through intentional misstatements, omissions, or falsification of accounting records—can mislead stakeholders, obscure financial risks, and result in regulatory breaches or reputational damage.

b) Controls

The Bank maintains a comprehensive set of internal controls to ensure the integrity, accuracy, and reliability of its accounting records and financial statements. These controls cover automated processes, manual validations, system interfaces, and governance mechanisms.

Most accounting entries are generated automatically through interfaces between the various product systems and the central accounting platform, with the IT monitoring these integrations and implementing controls to detect and address interface failures. Branches operate within autonomous accounting environments that communicate seamlessly with the Bank's central system, ensuring consistency across the organization.

In addition to automated processing, the Bank performs monthly reconciliations of bank accounts, suspense and clearing accounts, and product portfolios against accounting records. Manual accounting entries remain subject to strict oversight, requiring review and approval by a second staff member to maintain segregation of duties and ensure proper traceability.

Governance processes further reinforce the control environment. Monthly management accounts are reviewed and approved by the Executive Committee, while semi-annual and annual financial statements undergo review by the Executive Committee, the Board of Directors, and the Audit Committee. These financial statements are also subject to external audit by an independent auditor. Financial information produced through these controls supports both internal reporting and external regulatory disclosures. Business units receive monthly management reports, enabling them to review and challenge their financial results, thereby promoting accountability, transparency, and sound financial management.

c) Ownership

The Finance Department holds the primary ownership for the preparation, accuracy, and integrity of the Bank's financial statements. This includes ensuring compliance with applicable accounting standard, regulatory requirements, and internal financial controls.

Additional ownership is also provided by the following:

- Statutory Auditor in relation to revision of the Bank's financial statements, notably to provide independent assurance that the financial information presented is fair, accurate, and compliant with applicable accounting standards and regulatory requirements.
- Audit Committee which also issue an opinion on the process of revision of the Bank's financial statements.

5.2.8 Non-Financial Statements

a) Description

Non-financial statements are formal disclosures that provide information on the Bank's performance beyond financial metrics. These typically include the management of non-financial contracts — such as those involving suppliers, service providers, outsourcing arrangements, and sponsorships, data related to environmental, social, and governance (ESG) practices, risk management, corporate ethics, anti-corruption measures, and diversity and inclusion, among other matters.

b) Controls

The Bank ensures that non-financial disclosures are subject to proper validation, governance oversight, and audit review, in alignment with both internal standards and applicable regulatory frameworks.

c) Ownership

The primary ownership for the content and accuracy of non-financial statements lies with the Bank's Front Office areas. Each area is accountable for collecting, validating, and reporting accurate and complete non-financial data related to its operations, including information on compliance ESG practices, internal controls, contractual commitments, and risk management.

5.2.9 Cybersecurity

a) Description

Cybersecurity in banking is about securing the entire digital infrastructure of the Bank — from online banking systems to internal databases — against unauthorized access, data leaks, and malicious attacks. Effective IT security is critical for maintaining trust, compliance, and operational stability in an industry increasingly targeted by cybercriminals.

b) Controls

This matter is addressed under all regulations, procedures and operational manuals belonging to the IT Infrastructure Department, the IT Development and Application Support Department and the CISO Office.

While not exhaustive, a layered set of technical and organisational controls are in place, including system and infrastructure hardening, firewall and network security management, web application security, Anti-DDoS solutions, Security Operations Centre (SOC) and SIEM-based monitoring, robust access control and user-entitlement arrangements, and data encryption at rest and in transit, contributing directly

and indirectly to the protection of systems, data confidentiality and integrity, and overall operational resilience.

c) Ownership

The primary ownership for cybersecurity lies with each employee of the Bank and the first line of defense of the Bank's ICT function, specifically the Infrastructure Department and the IT Development and Application Support Department.

The CISO Office provides additional support on the monitoring of the necessary controls, as well as on the governance side.

5.3 OTHER INTERNAL RULES

While not identified as specific controls to address the types of fraud referred to in 5.2 above, there is a set of internal rules that indirectly play a very important role in preventing fraud events.

➤ Code of Conduct

Haitong Bank's Code of Conduct is a key tool in fostering a culture of integrity and legal compliance across the institution. It plays a critical role in fraud prevention by promoting adherence to the Bank's core values, principles, and legal obligations. The Code sets clear expectations for ethical behavior and reinforces the importance of accountability at all levels. By encouraging transparency, respect for rules, and responsible conduct, the Code helps to deter fraudulent and corrupt practices. This proactive approach ensures that ethical considerations remain central to the Bank's daily operations and that its corporate culture aligns with both regulatory requirements and the highest standards of governance.

➤ Communications Monitoring and Filing Regulation (document number R18)

The Communications Monitoring and Filing Regulation at Haitong Bank, S.A. plays a key role in fraud prevention by establishing internal rules for monitoring and recording communications related to business activities and operations. This Regulation helps detect suspicious behavior and irregularities early on by ensuring transparency and accountability in communications that may lead to transactions or constitute preparatory acts. These communications must be made by means that can be recorded, stored and monitored. This strengthens the Bank's ability to prevent and respond to potential fraud.

➤ Global Restrictions Regulation (document number R19)

The Global Restrictions Regulation at Haitong Bank, S.A. is a vital control mechanism that helps prevent fraudulent or unethical practices by imposing strict limitations on certain activities during sensitive investment banking transactions. These Restrictions—such as Research Restrictions, Proprietary Trading Blackout Periods, and Personal Account Dealing Blackout Periods—are designed to mitigate conflicts of interest and prevent the misuse of privileged or non-public information. By controlling when and how employees can act on specific issuers or transactions, the Regulation helps safeguard the integrity of the Bank's operations, ensuring that decisions are not influenced by insider information or personal gain. Additionally, by aligning with market standards and regulatory requirements, and enforcing consistent application across all Haitong Bank Group geographies, the Regulation strengthens internal governance and reinforces the Bank's defenses against fraudulent behavior.

➤ Information Classification Regulation (document number R17)

The Information Classification Regulation is a critical tool in the prevention of fraud by ensuring that all information assets—ranging from client data to internal documents and communications—are properly classified, protected, and managed. By establishing clear guidelines for handling sensitive information, this Regulation helps safeguard the confidentiality, integrity, and availability of data, reducing the risk of unauthorized access, manipulation, or disclosure. Through structured controls and employee accountability, the Regulation ensures that critical information is only accessible to authorized personnel, limiting opportunities for internal or external fraud. Additionally, the framework enables continuous monitoring and control of information flows, reinforcing the Bank's resilience against data breaches and fraudulent misuse of information.

➤ Market Control Regulation (document number R45)

The Market Control Regulation is a fundamental component in the Bank's defense against financial fraud, particularly in the context of market abuse. By establishing clear rules and procedures for monitoring securities market activities, the Regulation helps detect, prevent, and report suspicious behavior that could indicate market manipulation or insider trading. It ensures that the Bank, its employees, and governing bodies act with integrity and in full compliance with applicable laws across all jurisdictions. The Bank is equipped with the necessary tools and responsibilities to proactively identify and analyze potentially fraudulent transactions, whether executed in regulated markets or in over-the-counter (OTC). This regulation not only protects the Bank's reputation but also reinforces transparency and trust in the financial markets.

➤ Personal Data Privacy Regulation (document number R24)

The Personal Data Privacy Regulation plays a crucial role in fraud prevention, as it governs the lawful and secure processing of clients' and employees' personal data. By establishing clear guidelines for data collection and handling—based on legal obligations, contractual relationships, consent, and legitimate interests—the Regulation ensures that personal and financial information is properly safeguarded. This Regulation is especially relevant to fraud prevention in several critical areas. During client onboarding and throughout the Know Your Client (KYC) and Anti-Money Laundering (AML) processes, personal data is used to verify identities, screen against official watchlists, and detect anomalies. These procedures help prevent identity fraud and ensure that the Bank does not unknowingly facilitate illegal activity.

Additionally, the Regulation supports fraud prevention by enabling data analysis in financial due diligence, monitoring client operations, and ensuring proper risk management and audit controls.

By defining strict protocols for data use—whether processed internally or by third-party service providers—the Personal Data Privacy Regulation reduces the risk of data misuse and unauthorized access. This structured approach to data protection not only complies with legal requirements but also strengthens the Bank's ability to detect, prevent, and respond to fraud effectively.

➤ **Selection and Assessment of Management and Supervisory Body Members and Key Function Holders Policy (document number P06)**

The Selection and Assessment of Management and Supervisory Body Members and Key Function Holders Policy is a vital mechanism for fraud prevention, as it ensures that individuals in key functions and oversight positions possess the integrity, qualifications, and independence necessary to manage the Bank prudently and responsibly. By requiring ongoing assessments of fit and proper, professional qualification, independence, availability, and ethical standards - not only at the start of their appointment but throughout their term - this Policy helps safeguard the Bank from potential misconduct and governance failures. The Policy also includes measures to prevent, detect, and address conflicts of interest, which are critical in reducing opportunities for internal fraud or abuse of power. By setting a strong foundation for responsible leadership, this policy protects the Bank's operations, clients, and reputation from the risks associated with poor governance and fraudulent behavior.

➤ **Reporting of Wrongdoings (Whistleblowing) Regulation (document number R16)**

The Whistleblowing Regulation plays a fundamental role in the Bank's fraud prevention and detection framework. By establishing formal, confidential, and secure channels for the internal reporting of irregularities, it enables employees and other relevant stakeholders to report suspicions of fraudulent activities, corruption, or other violations of internal or legal provisions. This mechanism facilitates the early identification of potentially harmful conduct, allowing for timely investigation and mitigation. Moreover, by promoting a culture of transparency, ethical responsibility, and protection against

retaliation, the Regulation strengthens the integrity of the institution, reinforces internal control systems, and contributes to full compliance with regulatory requirements and best governance practices.

5.4 DETECTION, ANALYSES AND RESOLUTION

A risk-based approach is employed to proactively identify potential fraud and suspicious activities. This involves meticulously documenting the processes, technologies, and systems used to detect fraud.

To effectively identify fraudulent practices, controls have been implemented by the Bank that are proportionate to the level of identified fraud risk. This ensures preventative measures are aligned with potential threats. All detected fraud cases are managed according to internal processes and reviewed considering all available information to determine if it constitutes a potential fraud incident.

Haitong Bank maintains a comprehensive audit trail record for every analyzed fraud case, including the decisions made and actions taken to mitigate associated risk.

As part of Fraud Risk Prevention efforts, if there are suspicions of fraud incidents and if applicable, the Bank reports the incident to the authorities. An effective relationship with the authorities is also fostered, which facilitates information sharing, supports responses to fraud attacks, and enhances cooperation in investigating fraud cases. All the information requests from police authorities are addressed within the established timeframes.

5.4.1 Internal report

Employees on the front lines often have the best insights into operational weaknesses, process or technology vulnerabilities that could be exploited by fraudsters. An internal reporting channel allows them to flag these issues before they become major security breaches.

Timely internal reports enable the organization to investigate potential vulnerabilities or suspicious activities quickly. This rapid response can prevent a minor incident from escalating into a significant fraud event. Every reported incident, even if it doesn't lead to a confirmed fraud, provide valuable intelligence on emerging fraud trends, attack vectors, and weaknesses.

By addressing internally reported issues on fraud, the Bank continuously strengthens its overall security posture, making it a harder target for fraudsters. Addressing potential fraud issues internally before they become public can prevent the Bank and customer reputational damage.

Internal reporting act as an early warning system and a continuous improvement mechanism, strengthening the Bank defenses from the inside out, making it more resilient against fraud attempts.

5.4.2 External report

In parallel with the internal report referred above, and provided that the conditions referred to in the Reporting of Wrongdoings (Whistleblowing) Regulation are met, employees may also file external reports with the competent authorities for this matter, namely the:

- i. Public Prosecutor's Office (*Ministério Público*);
- ii. Criminal police bodies;
- iii. Bank of Portugal;
- iv. Independent administrative authorities;
- v. Public institutes;
- vi. General inspections and similar entities and other central services of direct administration of the State, endowed with administrative authority;
- vii. Local authorities;
- viii. Public associations.

5.5 MONITORING AND EVALUATION

5.5.1 Risk Assessment

The Bank regularly conducts a business risk assessment to evaluate its exposure to fraud. This assessment identifies inherent fraud risks, evaluates the effectiveness of existing controls, and highlights areas for improvement.

This risk assessment process systematically covers, at a minimum:

- a. identification of the risks in the Front Office areas based on its structure, products, services and distribution channels.
- b. identification of processes and controls in place to mitigate the risks.
- c. identification of gaps or weaknesses in the control structure facing the risks.

The Bank anti-fraud activities include targeted controls designed to mitigate the fraud risks identified during the fraud risk assessment process.

5.5.2 Limitations of Internal Controls

Internal controls alone will not prevent and detect all fraud. Additionally, there are several inherent limitations that can reduce the effectiveness of even well-designed internal control systems:

- *Human error*: The effectiveness of preventive controls is limited by human error, which can result from errors in judgment, unclear or misunderstood instructions, distraction, incompetence, or carelessness
- *Changes in operations or processes*: Changes in personnel or systems can result in breakdowns of internal controls. For example, downsizing might create a situation which remaining employees are unaware of internal controls that were previously in place. Consequently, management might design internal controls that are effective initially, but it should ensure these controls are periodically updated to keep pace with changing environment.
- *Circumvention*: Employees might look for ways to circumvent controls, particularly if these controls are new, cumbersome, or inconvenient.
- *Collusion*: This occurs when an individual works with one or more other parties, either inside or outside the organization, to circumvent controls. For instance, an accounts payable clerk and an employee responsible for initiating electronic payments could collaborate to create a fictitious vendor and then transfer funds to that vendor's supposed bank account.

5.5.3 Evaluation and effectiveness of controls

All Front office areas should conduct control tests to assess the suitability, design and operational effectiveness of their fraud systems and controls.

When incidents of fraud are detected, the Bank conducts root-cause analysis regarding the review of alerts, resolution and customer response. The results and conclusions of these analysis support changes to the controls or procedures and risk assessments carried out.

Fraud metrics are an essential tool for quantifying and reporting on the nature of the fraud risks the Bank is exposed to. Periodic and timely collection and analysis of the information are essential for effective management, reporting and supervision of fraud risks.

6. ARCHIVE

This Regulation, and all the documents associated, are subject to the general archiving rules laid down in the procedure LEG12.PM220 – Archive Management.

7. DISCLOSURE

This Regulation is available on the **Bank's intranet and corporate website** and any change to the same should be duly communicated by e-mail to all the Bank's employees.

8. CONTROL OF VERSIONS

Table 1: Information about the Document	
Name of the Document	Fraud Prevention Regulation of Haitong Bank, S.A.
Version	Version 1
Prepared by	Compliance Department
Endorsed by	Executive Committee on 09/04/2026
Approved by	Board of Directors on 25/06/2026

Table 2: Versions' update	
Approval and Update Date	Main Changes
Version 1.0 approved on 25/06/2026	Original Version

9. ANNEXES

9.1. Annex 1 – Fraud Prevention Responsibility Matrix

Action	Board	Management	Risk / Rating	Legal & Compliance	Internal Audit	Finance / Treasury	M&A / Capital Markets / Project Finance / Derivates	CISO/ IT / Online Banking	HR	Operations
1. Fraud Risk Management Oversight	P									
2. Fraud Prevention Controls (Process Level)		P	S	S	S	S	S	S	S	S
3. Fraud Risk Assessment		P	S	S	S	S	S	S	S	S
4. Fraud Detection Controls (Process Level)		P	S	S	S	S	S	S	S	S
5. Fraud Education / Training and Awareness		SR		SR				SR	SR	SR
6. Reporting of Concerns / Complaints / Violations	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR
7. Whistleblower Follow-up				P						

8. Fraud Prevention / Detection	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR
9. Proactive Fraud Auditing					P					
10. Internal Controls Review	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR
11. Disciplinary Actions		SR		SR					SR	

P (Primary Responsibility)

S (Secondary Responsibility)

SR (Shared Responsibility)