Prevention Plan of Corruption Risks and Related Offenses

CLASSIFICATION
Public

IDENTIFICATION

Version	Date	Created by:	Reviewed by:	Approved by:	Comment Review
PSA.0048.01	2022.08.22	Eduardo Cruz (RCC)	Renato Cardoso (CCID) Carina Ramos (FIN)	Renato Oliveira (CEO)	Original Version
PSA.0048.02en	2023.07.31	Eduardo Cruz (RCC)	Renato Cardoso (CCID) Carina Ramos (FIN)	Renato Oliveira (CEO)	Revision after Gap analysis PWC

Porto, 31st July 2023

Renato Oliveira

João Lima Pinto

ÍNDICE

SCOPE AND OBJECTIVE

In compliance with Decree-Law 109-E/2021, of December 9, ebankIT has decided to adopt a set of measures in the field of anti-corruption, highlighting the good practices already provided for in its Code of Ethics and Conduct, available at www.ebankit.com.

ebankIT also takes into account the International Standard NP ISO 37001:2018, structuring its measures in a continuous improvement cycle.

The law considers it essential to strengthen and enhance the mechanisms for preventing and detecting corruption and related crimes. Thus, the anti-corruption strategy identifies seven priorities for reducing the phenomenon of corruption.

ebankIT will ensure that it contributes to building a better society.

LEGAL TYPES AND OFFENCES

Under Decree-Law 109-E/2021, corruption and related offenses are defined as the following crimes (see List of Offenses attached):

1. Corruption;
2. Undue receipt and offering of an advantage;
3. Embezzlement;
4. Economic participation in business;
5. Concussion;
6. Abuse of power;
7. Prevarication;
8. Influence peddling;
9. Laundering or fraud in obtaining or diverting a subsidy, grant or credit.

ANTI-CORRUPTION COMPLIANCE OFFICER

ebankIT's Executive Committee has appointed the *Compliance and Continuous Improvement Director* - CCI Director as the Anti-Corruption Compliance Officer.

To this end, he has been given the responsibility and delegated the necessary authority to ensure the effective operation of the Corruption Prevention System, namely:

A. Executing, monitoring and reviewing the Prevention Plan of Corruption Risks and Related Offenses (PPCRRO);
B. Supervising the design and implementation of the Corruption Prevention System;

C. Providing advice and guidance on the Corruption Prevention System and issues associated with corruption;
D. Ensuring that the Corruption Prevention System complies with the requirements of the standard and applicable legislation; and,
E. Reporting on the performance of the Corruption Prevention System to the Executive Committee.

EBANKIT'S ACTIVITY

ebankIT is a FinTech software company that develops an omnichannel platform for the banking sector to enable banks and other financial institutions, such as credit unions, to innovate and adapt quickly to the demands of the digital transition. The ebankIT digital platform has helped financial institutions around the world quickly implement banking solutions for their clients and internal teams.

There are currently more than 100 full-time employees at ebankIT. The ebankIT portfolio comprises the following components: Internet Banking, Mobile Banking, Wearable Banking, Branch Front Office, Contact Center, Account Opening, Social Banking, Voice Banking, Augmented Reality, Analytics, Campaigns Management, among others.

ASSESSMENT OF RISKS OF CORRUPTION AND RELATED OFFENCES

ebankIT's Prevention Plan of Corruption Risks and Related Offenses (PPCRRO) establishes the principles, guidelines and responsibilities for proper risk identification, analysis, classification, treatment and response. It promotes the broadening of the scope of analysis and assessment of the risk of corruption, thus involving all units of the internal organizational structure.

Its purpose is to create and protect value, improve performance, support decision-making and the achievement of objectives by mitigating situations that could expose ebankIT to acts of corruption and related offenses. It applies to the different levels of risk to which ebankIT is exposed.

GUIDING PRINCIPLES

Each area must be responsible for managing, identifying, monitoring and periodically updating its risks, reviewing the assessment made of the impact and probability of occurrence.
The risk management process is a continuous and systematic process, since new risks may arise, and existing ones may change or cease to be relevant.
To improve the risk management model, the methodology used is reviewed and the criteria and parameters used are reassessed on an annual basis. The aim is to achieve an increasingly effective and robust model.

The communication process supports and facilitates the most effective application of risk management. Sharing timely and relevant information is fundamental to raising awareness and empowering the entire organization and thus promoting the dissemination of the risk culture, as well as accountability for risks and internal controls.

Principles for the internal governance of risk management:

The Executive Committee is responsible for approving and periodically reviewing ebankIT's general strategies and relevant policies. To this end, it must:

- Understand the major risks occurring and establish acceptable levels for such risks;
- Approve the organizational structure that clearly determines responsibilities, powers and reporting lines; and,
- Ensure that the Heads of Departments take the necessary steps to identify, measure, monitor and control such risks.

The Executive Committee is ultimately responsible for ensuring that adequate internal control is established and maintained.
The *Heads of Departments* are responsible for:

- Implementing strategies and policies approved by the Executive Committee;
- Developing processes to identify, measure, monitor and control risks;
- Maintaining an operational organizational structure and ensuring that delegated responsibilities are effectively fulfilled;
- Establishing appropriate internal control policies and monitoring the adequacy and effectiveness of the internal control system.

The Executive Committee and the *Heads of Departments* have a responsibility to promote high standards of ethics and integrity and to establish a culture in the organization that shows and demonstrates to all employees and at all levels the importance of internal controls.

All ebankIT employees must understand their role in internal control processes and must be involved.

CONTROL ACTIVITIES AND SEGREGATION OF DUTIES

Control activities are an integral part of the day-to-day activities at ebankIT.
Effective internal control requires control activities to be defined at all business levels.
This control structure should include:

- Top-level reviews;
- Appropriate control activities for different areas;
- Physical controls;
- Checks on compliance with exposure limits and follow-up of non-compliance situations;
- A system of approvals and authorizations; and,
- A verification and reconciliation system.

Effective internal control requires that there is an adequate segregation of duties and that employees do not have responsibilities assigned in a situation of conflict of interest.

The areas with potential conflicts of interest are identified in HRM.0032 - Segregation of duties matrix.

On the other hand, effective internal control requires the availability of adequate and complete financial operating information, as well as external data and information on events and conditions relevant to the decision-making process. The information must be reliable, timely and accessible and must also be available in a consistent form. This information is accessible at Sharepoint\FINDD\Area.

The financial controls implemented to ensure the proper management of financial transactions are:

- Segregation of duties, so that the same person cannot propose and approve a payment;
- Appropriate authorization levels for approving payments (so that the highest transactions require approval by the Executive Committee);
- Obligation to affix at least two signatures to payment approvals;
- Obligation to attach appropriate supporting documentation to payment approvals;
- Restriction on the use of cash and implementation of effective cash control methods;
- Requirement for periodic management review of significant financial transactions; e,
- Implementation of periodic and independent financial audits.

The non-financial controls implemented to help ensure the proper management of purchases, operations and other non-financial aspects are:

- Selecting of contractors, subcontractors, suppliers and consultants who have been subject to a prior evaluation process, in which the possibility of their involvement in cases of corruption is assessed;
- Assessment of the need and legitimacy of the services to be provided to the organization by a business partner, when deemed necessary (excluding clients);
- Assessment of the adequate provision of services;
- Assessment of the reasonableness and proportionality of any payments to be made in respect of the services awarded. This is particularly important to avoid the risk of the business partner using part of the payment to make a bribe on behalf of or in the interests of ebankIT;
- Awarding contracts, whenever possible and reasonable, only after the number of bids defined in the Third-Party Management Policy - PSA.0006 has been submitted;
- Obligation to have at least two people evaluating the bids and approving the award of a contract (Board Members);
- Implementation of a segregation of duties, so that the person who authorizes the award of the contract is different from the person who requested the purchase order; and,
- More demanding management supervision of transactions that potentially pose a high risk of corruption.

INFORMATION AND COMMUNICATION

Efficient internal control requires effective communication channels in order to ensure that all employees clearly understand and adhere to the policies and procedures that affect their duties and responsibilities, and that any other relevant information reaches the appropriate recipients.

The policies and procedures are available on the ebankIT website at www.ebankit.com.

Whenever necessary, *sharing sessions* are held to remind people of these rules.

In the process of *onboarding* new employees, it is part of the process to make them aware of these rules in order to keep the controls active.

INTERNAL CONTROL AND RISK MANAGEMENT

1st line of defense: *Heads of Departments and Team Leaders*

As the first line of defense, *Heads of Departments and Team Leaders* manage risks and have responsibility for them. They are also responsible for implementing corrective actions to resolve deficiencies in processes and control mechanisms.

This 1st Line identifies, assesses, controls and mitigates risks, outlining the implementation of internal policies and procedures to ensure that activities are carried out in accordance with established goals and objectives.

Through the implementation of the controls, cases of non-compliance can be identified. Potentially identified situations should be referred to the Compliance and Continuous Improvement Department (CCID), to compliance@ebankit.com.

2nd Line of Defense: Risk Management

The Finance Department is responsible for *Enterprise Risk Management* (FIN.0011), in which it identifies, assesses and controls, in a global and integrated manner, the risks associated with ebankIT's activities, and for the corruption risk matrix in the Annex to this document, in order to ensure that the risks remain at controlled levels for ebankIT.

The *Finance Department* interacts with the *Compliance* and *Continuous Improvement* Department to ensure appropriate policies, procedures and controls.

The risk management policy and methodology are adjusted to the nature and mission of ebankIT and take into account international standards, policies and good practices.

3rd line of defense: Internal Audit

Internal audits are coordinated by the *Compliance* and *Continuous Improvement* Department. Internal audit is responsible for auditing compliance with established controls.

Internal audit is an independent and impartial activity in relation to other departments and units, with a direct reporting line to the Executive Committee, and which aims to ensure, in an impartial manner, the effectiveness, operability, security and compliance of services, systems, processes and activities.

All areas of ebankIT's activity are susceptible to internal auditing, but it is preferably directed at the units, activities, processes and systems that pose the greatest potential risk, in order to give priority

to preventing the most significant risks, inherent to the complexity and dynamics of accelerated change that characterize the context of ebankIT's activity.

ADEQUACY OF RISKS AND MEASURES IMPLEMENTED

The risk management matrix for corruption and related offenses described in the Appendix complements the risks defined in *Enterprise Risk Management* (ERM) FIN.0011.

ANNEX

Caption:

S - Severity

1 - Insignificant; 2 - Limited; 3 - Significant; 4 - High.

P - Probability

1 - Rare; 2 - Occasional; 3 - Frequent; 4 - High.

Risk level = G*P

1 to 3 - Very Low; 4 - Low; 6 - 9 Medium; 12 - 16 High (High or maximum)

	Inherent risk					**Residual risk**			
Ativity	**Risk**	**Prevention Measures**	**S**	**P**	**Risk Level**	**Additional measures**	**S**	**P**	**Nível de Risco**
Procurement of goods and services	Not choosing the best option for the supply of goods or services; influence and favoring/favoring of the entities involved with the aim of obtaining own gains and benefits.	1. Third party management policy. 2. Finance Procedures. 3. EbankIT Code of Ethics and Conduct.	4	2	Medium	Awareness-raising through training for *Heads of Departments*.	2	1	Very Low
	Influence of suppliers (goods and/or services) on the structure and favoritism of the entities involved in the contracts awarded.	1. *Third Party Management Policy*. 2. *Finance Procedures*. *3. EbankIT Code of Ethics and Conduct.*	4	2	Medium	Consciencialização por via de formação dos *Heads of Departaments*.	2	1	Very Low
Supplier monitoring	Not following the internal *workflow* defined in the Third party management policy.	*1. Third Party Management Policy.* *2. Finance Procedures.*	4	2	Médio	Awareness-raising through training for *Heads of Departments.*	4	1	Low

		3. EbankIT Code of Ethics and Conduct. *4. Awareness.*							
	Failure to take legal / regulatory requirements into account in the supplier management process.	*1. Third Party Management Policy.*	4	2	Medium	Awareness-raising through training for Heads of Departments.	4	1	Low
	Acceptance of benefits to give advantages to oneself or a third party.	1. Third Party Management Policy. 2. Finance Procedures. 3. EbankIT Code of Ethics and Conduct. 4. Awareness.	4	2	Medium	Awareness-raising through training for Heads of Departments.	4	1	Low
Cash management/ funds	Undue access to funds in bank accounts and appropriation of amounts by falsifying/ tampering with documents.	*1. Finance Procedures.* *2. Incident Response Plan.*	4	2	Medium	N/A	4	2	Medium
Reporting activities	Adulteration of basic information for budget execution (budget monitoring).	1. monthly submission of the budget execution file to the areas for validation.	3	1	Very Low	N/A	3	1	Very Low
Audit activities	Potential loss of independence and objectivity, devaluation of evidence of wrongdoing, collusion/cover-up of irregular practices.	1. adoption of Internal Audit methodology in accordance with ISO 19011. 2. Review of audit reports and conclusions (*4 eyes principle*).	4	1	Low	N/A	4	1	Low
Information Security Management	Improper access to confidential information in the context of financial proposals.	1. controls within the scope of ISO/IEC 27001. 2. SOC 2 Type 2 report.	3	1	Very Low	N/A	3	1	Very Low

	Dependence on critical suppliers.	Monitor activities by auditing critical suppliers.	4	2	Medium	N/A	4	2	Medium
	Vulnerabilities in confidentiality, integrity and availability of Information Security.	Maintenance of the information security system in accordance with ISO/IEC 27001.	4	2	Medium	Training actions to strengthen awareness and knowledge of best practices related to cybersecurity.	3	1	Very Low
	Fuga e divulgação indevida de informação para o exterior.	1. Manutenção do sistema de segurança da informação de acordo com ISO/IEC 27001. *2. Incident Response Policy and Plan.*	3	1	Muito Baixo	N/A	3	1	Very Low
Functioning of the Board of Directors	Use or disclosure of privileged and/or confidential information for its own benefit and/or that of a third party.	1. Recording of analyses, proposals and resolutions of the Board of Directors. 2. Signature of the minutes of the Board of Directors' meetings by all members present.	3	1	Very Low	N/A	3	1	Very Low
	Acceptance of benefits for the attribution of advantages to oneself or a third party	1. Recording the analyses and proposals and resolutions of the Board of Directors Minutes. 2. Signature of the minutes of the Board of Directors meetings by all members present.	3	1	Very Low	N/A	3	1	Very Low

	Omission/manipulation/adulteration of information with the aim of prejudging decisions.	1. Recording of the Board's analyses and proposals and deliberations in the minutes. 2. Signature of the minutes of Board meetings by all members present.	3	1	Very Low	N/A	3	1	Very Low
Human Resources Management (Recruitment processes)	Acceptance of benefits for the attribution of advantages to oneself or a third party.	1. ebankIT Code of ethics and conduct. 2. Awareness raising.	3	1	Very Low	N/A	3	1	Very Low
	Use or disclosure of privileged and/or confidential information for own benefit and/or that of a third party.	1. ISO/IEC 27001 controls. 2. ebankIT Code of ethics and conduct. Awareness raising.	3	1	Very Low	N/A	3	1	Very Low
Managing the performance appraisal and progression process	Acceptance of benefits for the attribution of advantages to oneself or a third party.	1. ebankIT code of ethics and conduct. 2. Awareness raising. 3. Monitoring of the process by HR and with the approval of the Executive Committee.	3	1	Very Low	N/A	3	1	Very Low
	Omission/manipulation/adulteration of information in order to influence decisions.	1. ebankIT Code of ethics and conduct. 2. Awareness raising. 3. Monitoring of the process by HR and with the approval of the Executive Committee.	3	1	Very Low	N/A	3	1	Very Low
Cash flow Management	Undue transfers/payments 1. Finance procedures	1. Finance procedures.	4	1	Low	N/A	4	1	Low

Business with sanctioned countries.	Risk of doing business with sanctioned countries Policy 4 1 Low Review of Anti-Money Laundering Policy	Due Diligence in accordance with Third Party Management	4	1	Low	Review of the Anti-Money Laundering Policy	3	1	Very Low
Business relations with natural/collective persons from countries with a high level of corruption	Risk of establishing corrupt relationships	1. Due diligence in accordance with the Third Party Management Policy 2. ebankIT Code of ethics and conduct. 3. Awareness raising.	4	1	Low	Review of the Anti-Money Laundering Policy	3	1	Very Low
Relationship with public officials and/or PEPs	Media exposure that could influence reputation.	1. Due Diligence in accordance with the Third Party Management Policy.	4	1	Low	Implement anti-corruption and conflict of interest policy. 2. Report all interactions with Public Agents and Politically Exposed Persons; 3. Signing a declaration that there is no conflict of interest; 4. Analysis of the declaration of conflict of interest of (PPEs), close members or persons closely associated with PEPs - Employees and candidates for employees. Employees and prospective employees.	3	1	Very Low

						5. Review of the Anti-Money Laundering Policy.			
Accepting offers, invitations	Influencing decisions.	1. ebankIT Code of ethics and conduct. 2. Raising awareness.	3	1	Low	1. Implement anti-corruption and conflict of interest policy.	3	1	Low
Allocating offers, invitations	Influencing decisions.	1. ebankIT Code of ethics and conduct. 2. Raising awareness.	3	1	Low	1. Implement anti-corruption and conflict of interest policy.	3	1	Low
Allocation of donations, partnerships and sponsorships.	Influencing decisions.	1. ebankIT Code of ethics and conduct. 2. Raising awareness.	3	1	Low	1. Implement anti-corruption and conflict of interest policy.	3	1	Low