Annual Report on Prevention Plan of Corruption Risks and Related Offenses 2025

7 of April 2025

INFORMATION CLASSIFICATION

Public

IDENTIFICATION

Version	Date	Issued by	Reviewed by	Approved by	Revision comments
PSA.0058.01	2023.04.08	Eduardo Cruz (RCC)	Renato Cardoso (CCID)	Renato Oliveira (CEO)	Original Version
PSA.0058.02en	2023.04.10	Eduardo Cruz (RCC)	Renato Cardoso (CCID)	Renato Oliveira (CEO)	(Translation from PT)
PSA.0058.03en	2024.04.22	Tânia Almeida (RCC)	Renato Cardoso (CCID)	Renato Oliveira (CEO)	Review of the Annual Risk Assessment Report on Corruption and Related Offenses
PSA-0058.04en	2025.04.07	Ana Carvalho (RCSC)	Renato Cardoso (CCID) Carina Ramos (FIN)	Renato Oliveira (CEO) João Pinto (Board member)	Annual revision.

Porto, 7th April 2025

Renato Oliveira

Name: Renato Oliveira

Title: CEO

João MR Lima Pinto

Name: João Lima Pinto

Title: Board Member

Table of Contents

Scope And Objective

On December 9, 2021, Decree-Law 109-E/2021 (“Decree-Law”) was published in the Official Gazette, creating the National Anti-Corruption Mechanism (“MENAC”) and approving the General Regime for the Prevention of Corruption (“RGPC”).

In accordance with Decree-Law 109-E/2021 of December 9, ebankIT has drawn up the Prevention Plan of Corruption Risks and Related Offenses (PPCRRO).

According to Article 6(4) of the “General regime for the prevention of corruption”, published in the annex to Decree-Law 109-E/2021 of December 9, the implementation of the PPCRRO is subject to monitoring, conducted as follows:

a) Preparation, in October, for an interim assessment report on situations identified as high or maximum risk.
b) Preparation, in April of the following year, of an annual assessment report, including quantification of the degree of implementation of the preventive and corrective measures identified, as well as a forecast of their full implementation.

In this context, ebankIT presents its annual assessment report specifying the level of implementation of the preventive and corrective measures identified and their expected full implementation.

The revision of the PPR is the result of an extensive analysis of the whole of ebankIT in which the risks in each of the organization's areas of activity were identified, as well as the preventive and corrective measures to mitigate these risks. ebankIT presents its annual evaluation report specifying the level of implementation of the preventive and corrective measures identified and their expected full implementation.

This report is published on the official website www.ebankit.com within 10 days of its implementation and any revisions or drafting.

Monitoring

The risk management for corruption and related offenses complements ebankIT's Enterprise Risk Management (FIN.0012.08) and Enterprise Risk and Opportunities Matrix (FIN.0012.08).

The purpose of the assessment was to conclude on the existence or otherwise of the preventive measures indicated in the PPCRRO and their evidence. This monitoring was not intended to test the design and operational effectiveness of the preventive measures implemented, since this will be part of the internal audit activity.

It should be noted that, following the GAP analysis on the Anti Financial Crime System carried out in 2023, the risk prevention and treatment measures provided for in the PPCRRO were evaluated.

In the current PPCRRO, 44 risks were identified, of which, after the application of preventive measures, 2, was classified as medium risk, 21 as low and 21 as very low.

As a result of the monitoring carried out:

- The Prevention Plan for corruption risks and related offenses was revised on 24th March 2025.
- No incidents were reported in 2024.
- There were no significant changes regarding internal processes.
- Internal audit was initiated but wasn't completed during 2024. In 2025 it will be finished by 2Q2025.
- ISO/IEC 27001:2022 transition plan was completed at 1Q2025.

ebankIT's existing control instruments are:

- The Code of Ethics and Business Conduct, revised in 2023, includes a set of ethical and deontological rules to be observed in the daily activity of its employees in line with new legal requirements.
- Anti-Money Laundering Policy, which recognizes ebankIT's concern with fraud and money laundering issues, especially considering it operates in a highly regulated market like banking.
- Third Party Management Policy, with the aim of systematizing the workflow for selecting and contracting with suppliers, with considerations relating to risk analysis and due diligence already in place.
- Vendor Risk Assessment, a questionnaire due diligence sent to our partners and suppliers analyzing issues such as information security, cybersecurity, privacy, social and environmental responsibility.
- An established whistleblower mechanism that allows employees to report any suspicious activities or violations anonymously and without fear of retaliation. A whistleblowing channel is available on the ebankIT website.
- Policy on Anti-Corruption and Conflict of Interest Prevention.

Reporting

No incidents were reported in 2024. However, ebankIT has a reporting channel which has been publicized internally and is available to anyone from ebankIT's website.

Final Considerations

Internal audit conclusions will reflect the level of compliance of policies and procedures and allow us to conclude if the control measures adopted in the PPCRRO are efficient to ensure compliance with policies and procedures established. After that clear performance metrics should be implemented to evaluate the effectiveness of anti-corruption measures and controls.

Summary Of Risks

There are several common risks that cut across the entire structure of the organization, as shown in the table below.

Risks	Prevention Measures	Annual Assessment

Bribery and Corruption
• Acceptance of benefits for personal or third-party advantages.
• Influencing decisions through bribery and favoritism.
• Lobbying for favors and trading influence.
• Establishing corrupt relationships, including money laundering.
	• Employees who are faced with a situation that could constitute a conflict of interest must request a waiver on the grounds of legal impediment.
	• assuming that they must report this situation under the terms defined in the following ebankIT policies:
	  • Code of Ethics and Conduct;
	  • AML Policy;
	  • information security policies and procedures;
	  • implementation of a whistleblowing channel;
	  • due diligence and third-party management policy.
	• Code of Ethics and Conduct.
	• Anti-fraud and Money Laundering Policy.
	• Rules of Use of Information System and Detailed Security policies, respectively.
	• Whistleblowing Channel implemented.
		• No issue was reported through reporting channel and there are no signs of suspicious activities.
		• 2Q2025 Internal audit should conclude about the level of controls implementation.

Information Security and Confidentiality • Theft of intellectual property. • Improper access to and disclose confidential information. • Manipulation of code and algorithms. • Vulnerabilities in information security. • Phishing and social engineering attacks.		
Fraud and Financial Misconduct • Adulteration of budget information. • Fraudulent invoicing and transactions. • Misleading marketing practices. • Overpaying for goods and services. • Use of unlicensed software.		
Compliance and Legal • Failure to comply with legal and regulatory requirements. • Financial penalties due to breaches. • Risks associated with doing business with sanctioned countries.		
Operational • Dependence on critical suppliers. • Influence and favoritism in supplier management.		

• Service interruptions and suppression of activities. **Reputational** • Media exposure affects reputation. • Reputational damage from breaches and inadequate responses. **Governance and Oversight** • Bias and favoritism in appraisals. • Lack of oversight and transparency. • Potential loss of independence and objectivity.	• Revision of Enterprise Risk Management (ERM). • Analysis of suppliers carried out in the management system review. • Revision and approval of ISMS in accordance with ISO 27001:2022	

Table 1 - Risk Summary

The measures to be implemented in 2025 have been established, as set out in the table below.

Risks and Prevention Measures

	Inherent Risk					Residual Risk				Annual Review		
Activities	Risk	Preventive measures	G	P	Risk Level	Additional measures	G	P	Risk Level	Measures planned for 2024	Level of realization of measures 2024	Measures planned for 2025
Auditing activities	Potential loss of independence and objectivity, devaluation of evidence of wrongdoing, collusion/cover-up of irregular practices. Bias in audit findings. Inadequate audit procedures. Failure to detect corruption.	1. Adoption of Internal Audit methodology in accordance with ISO 19011. 2. Review of audit reports and conclusions (4 eyes principle).	4	2	Medium	Audit Reports should be validated by CCI and Finance.	4	1	Low	N/A	N/A	Perform internal audit. Internal audit results analysis to feel the efficiency and assess the need to have specific training or hire external audit.
Cash/fund management	Undue transfers/payments; fraudulent transactions; money laundering	1. Finance Procedures. 2. Incident Response Plan.	4	2	Medium	Not applicable	4	2	Medium	Perform Anti-Corruption and Conflict of Interest Policy internal audit.	In preparation.	Perform internal audit.to financial procedures
Information Security and	Improper access to confidential	1. Controls within the scope of	3	1	Very Low	Not applicable	3	1	Very Low	Maintain the established	Being implemented	Implement the controls

	Inherent Risk					Residual Risk				Annual Review		
Activities	Risk	Preventive measures	G	P	Risk Level	Additional measures	G	P	Risk Level	Measures planned for 2024	Level of realization of measures 2024	Measures planned for 2025
Privacy Management	information in the context of financial proposals.	ISO/IEC 27001 2. SOC 2 Type 2 report								processes and strengthen cybersecurity controls with the planned investments and adaptation of controls to the requirements of ISO/IEC 27001:2022.	(90%): Policies reviewed in accordance with 27001:2022.	according with the approved action plan
Information Security and Privacy Management	Dependence on critical suppliers	Monitor activities by auditing critical suppliers	4	2	Medium	Supplier Management Policy Review	4	1	Low	Perform Anti-Corruption and Conflict of Interest Policy internal audit.	Partially realized (20%)	Conclude internal audit
Information Security and Privacy Management	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 activities to increase awareness and knowledge of the best	3	1	Very Low	Information security investment plan execution.	Being implemented (75%):	Conclude Information security investment plan

	Inherent Risk						Residual Risk			Annual Review		
Activities	Risk	Preventive measures	G	P	Risk Level	Additional measures	G	P	Risk Level	Measures planned for 2024	Level of realization of measures 2024	Measures planned for 2025
						practices in cybersecurity.						
Information Security and Privacy Management	Phishing and Social Engineering Attacks	Awareness and training.	4	2	Medium	Training exercises.	4	2	Medium	Phishing exercises.	Done (100%)	More Phishing exercises and awareness.
Information Security and Privacy Management	Leakage and improper disclosure of information.	1. Maintenance of Information Security System in accordance with ISO/IEC 27001. 2. Maintenance of a Privacy System in accordance with ISO/IEC 29100. 3. Incident Response Policy and Plan.	3	2	Medium	Reinforce DLP controls	3	1	Very Low	Restrict SW installation rules and increase BitLocker activation. Review web filter rules.	Being implemented (90%): Reviewed in accordance with 27001:2022.	Implement the controls according with the approved action plan
Information Security and Privacy Management	Financial penalties as result of breaches, inadequate or untimely response to the exercise of rights.	1. Maintenance of Information Security System in accordance with ISO/IEC 27001.	3	2	Medium	Training actions to strengthen awareness and knowledge of best practices	3	1	Low	Keep improving awareness and controls	Awareness session about phishing and password management	Keep doing awareness sessions and training employees

Activities	Inherent Risk Risk	Preventive measures	G	P	Risk Level	Residual Risk Additional measures	G	P	Risk Level	Annual Review Measures planned for 2024	Level of realization of measures 2024	Measures planned for 2025
		2. Maintenance of a Privacy System in accordance with ISO/IEC 29100. 3. Incident Response Policy and Plan. 4. Data subjects requests' response policy.				related to cybersecurity and privacy.						
Information Security and Privacy Management	Suppression of activities: by intervention of control authorities, incidents, attacks.	1. Maintenance of Information Security System in accordance with ISO/IEC 27001. 2. Maintenance of a Privacy System in accordance with ISO/IEC 29100. 3. Incident Response Policy and Plan and Business Continuity Plan.	3	2	Medium	Training actions to strengthen awareness and knowledge of best practices related to cybersecurity and privacy.	3	1	Low	Maintain the established processes and strengthen cybersecurity controls with the planned investments and adaptation of controls to the requirements of ISO/IEC 27001:2022	Being implemented (90%): Policies reviewed in accordance with 27001:2022	Implement the controls according to the approved action plan

	Inherent Risk					Residual Risk				Annual Review		
Activities	Risk	Preventive measures	G	P	Risk Level	Additional measures	G	P	Risk Level	Measures planned for 2024	Level of realization of measures 2024	Measures planned for 2025
Procurement of goods and services	Failing to choose the optimal option for supplying goods or services to the company, while influencing or favoring certain entities to gain personal benefits or advantages.	1. Supplier Management Policy. *2.* Finance Procedures. *3.* Code of Conduct and Ethics.	4	2	Medium	1. Revision of the *Supplier Management Policy*. Awareness-raising through training for department heads.	2	1	Very Low	Perform Anti-Corruption and Conflict of Interest Policy internal audit.	Partially realized (20%)	Conclude internal audit.
Procurement of goods and services	Influence of suppliers (goods and/or services) on the organizational structure and favoritism toward the entities involved in awarded contracts.	1. Supplier Management Policy. *2.* Finance Procedures. *3.* Code of Conduct and Ethics.	4	2	Medium	Revision of the Supplier Management Policy. Awareness-raising through training for department heads.	2	1	Very Low	Perform Anti-Corruption and Conflict of Interest Policy internal audit.	Partially realized (20%)	Conclude internal audit.
Procurement of goods and services	Overpaying for goods and services; non-competitive contract.	1. Third parties management policy. 2. Finance Procedures. 3. ebankIT Code of Ethics and	4	2	Medium	Awareness-raising through training for Heads of Departments.	2	1	Very Low	Perform Anti-Corruption and Conflict of Interest Policy internal audit.	Partially realized (20%)	Conclude internal audit

Activities	Inherent Risk					Residual Risk				Annual Review		
	Risk	Preventive measures	G	P	Risk Level	Additional measures	G	P	Risk Level	Measures planned for 2024	Level of realization of measures 2024	Measures planned for 2025
		Business Conduct.										
Report activities	Adulteration of basic information for budget execution (budget monitoring).	1. Sending the monthly budget execution file to each department for review and validation.	3	1	Very Low	Not applicable	3	1	Very Low	Perform Anti-Corruption and Conflict of Interest Policy internal audit.	In preparation.	Perform internal audit to financial procedures.
Supplier monitoring	Not following the internal workflow defined in the Third-parties management policy.	1. Third Parties Management Policy. 2. Finance Procedures. 3. ebankIT Code of Ethics and Business Conduct. 4. Awareness. 5. Annual internal audit	4	2	Medium	Awareness-raising through training for Heads of Departments.	4	1	Low	Perform Anti-Corruption and Conflict of Interest Policy internal audit.	Partially realized (20%)	Conclude internal audit
Supplier monitoring	Failure to take legal / regulatory requirements into account in the supplier management process.	1. Third Parties Management Policy. 2. Annual internal audit.	4	2	Medium	Awareness-raising through training for Heads of Departments.	4	1	Low	Perform Anti-Corruption and Conflict of Interest Policy internal audit.	Partially realized (20%)	Conclude internal audit

	Inherent Risk						Residual Risk				Annual Review		
Activities	**Risk**	**Preventive measures**	**G**	**P**	**Risk Level**	**Additional measures**	**G**	**P**	**Risk Level**	**Measures planned for 2024**	**Level of realization of measures 2024**	**Measures planned for 2025**
Supplier monitoring	Acceptance of benefits to give advantages to oneself or a third party.	1. Third Parties Management Policy. 2. Finance Procedures. 3. ebankIT Code of Ethics and Business Conduct. 4. Awareness. 5. Segregation of functions.	4	1	Low	N/A	4	1	Low	N/A	In preparation: Identification of the need for training	Training of Heads of Departments Heads Awareness on 9 December - International day against corruption

Table 2 - Risks and Preventive Measures

LEGEND:
G: Severity [1 - Insignificant - 2 - Marginal - 3 - Considerable - 4 - Significant]
P: Probability [1 - Rare - 2 - Occasional - 3 - Frequent - 4 High]
Risk Levels: [Low - 1 to 5] [Moderate - 6 - 10] [High - 11 - 15] [Very High - 16 - 20]

Level of Implementation:

In progress	0%	The Document/Template/Activity is under development
In preparation	15%	The document is being drafted / The activity is being planned/prepared
Under review	40%	The document is being revised / The supports for the activity are being developed
Being approved	50%	The document is in its final version but lacks approval / The activity is under approval
Being implemented	80%	The Document is approved and publicized / The activity is being implemented