NOVABASE

INTERIM EVALUATION REPORT

PLAN FOR THE PREVENTION OF RISKS OF CORRUPTION AND RELATED OFFENCES

LISBON

OCTOBER 2024

NOVABASE

NOVABASE

1. Background

On December 2021, Novabase approved the Plan for the Prevention of Risks of Corruption and Related Offences[1] (or "Plan") applicable to the universe of companies within Novabase Group (or "Novabase")[2] and addressed to all its *stakeholders*[3].

In the preparation of this Plan, the measures included in the 2021-2024 National Anti-Corruption Strategy, Studies, Reports and Recommendations published in this regard, as well as the domestic and international best industry practices, including the Requirements and Recommendations of Portuguese Standards ISO 31000 (Risk Management) and ISO 37001 (Anti-Corruption Management Systems) were considered.

1.1. Scope, Objectives and Methodology

1.1.1.1. Scope

The Plan for the Prevention of Risks of Corruption and Related Infractions covered all areas and segments of Novabase's activity, employees, suppliers and service providers.

1.1.1.2. Purpose

In the preparation of such Plan, the following purposes were set:

- Identifying risks of corruption and related offences or conflicts of interest in relation to each process or area;
- Determining specific measures to be implemented in order to prevent their occurrence; and
- Determining those in charge of supervising and monitoring the Plan.

1.1.1.3. Methodology

We started by seeking to define the concept of risk and map the processes and/or areas at Novabase which, in our view, would fall within the notion of risk.

We have identified the entities in charge of these processes and/or areas.

[1] This document was approved before the entry into force of Decree-Law No. 109-E/2021, of 9 December, which (i) created the National Anti-Corruption Mechanism ("MENAC"), an independent administrative entity whose mission is to promote transparency and integrity in public action and ensure the effectiveness of policies to prevent corruption and related offences, entity with powers of initiative, control and sanction and (ii) established the general regime for the prevention of corruption ("General Regime for the Prevention of Corruption").

[2] Meaning Novabase – Sociedade Gestora de Participações Sociais, S.A. and the companies that form part of the Novabase Group.

[3] Entities whose interests are involved in the corporate activity of Novabase Group, namely shareholders and investors, customers, suppliers and other business partners and all their employees.

And finally, we have identified the internal risk prevention and control measures and defined the ways in which the measures implemented or to be implemented were to be monitored and their periodic evaluation.

1.2. Processes, areas and responsibilities

Taking into account Novabase's functions and internal organization, we have identified and characterized potential situations involving the risk of corruption and related offences by areas and processes, categorizing these risks on a scale (low, moderate and high risk) according to the likelihood of their occurrence and respective impact.

There are several factors which can lead to a higher or lower degree of risk on a given area or activity, including:

- The probity of those involved;
- The legitimacy and legality of the acts and actions;
- The ethical commitment; and
- The quality and effectiveness of the internal control system.

While identifying the areas and processes capable of generating risks, the risks have been contemplated in abstract vis-à-vis their impact and likelihood of occurrence:

	Impact	Likelihood
Low	Does not result in financial losses, nor do the offences cause relevant damage to Novabase's image and ability to operate	Arises from a process that will only result from exceptional circumstances
Moderate	May result in financial losses, and disturbs Novabase's regular functioning	Associated with a sporadic process expected to occur over the course of the year
High	May result in major financial losses, harming Novabase's credibility	Arises from a current and frequent organizational process

In Annex II of the Plan, we have identified, in view of Novabase's internal organization, the areas and processes capable of generating risks, while also listing the risk situations and the respective responsible area.

1.3. Internal risk control and prevention measures

The internal risk control and prevention measures shown in Annex II have been delimited according to key processes and underlying risk situations, while also specifying the internal areas or departments in charge of their implementation, oversight and/or monitoring.

2. Interim Evaluation

The purpose of this Report is to fulfil the obligation established in Article 6(4)(a) of the General Regime for the Prevention of Corruption, reporting on the implementation of the preventive measures identified in the Plan for the Prevention of Risks of Corruption and Related Offences as being of high or maximum risk, as well as reporting on their evolution, in a logic of continuous improvement.

Two areas where there were high risk situations were identified, namely Technological Infrastructures and Communications, both under the responsibility of the Information Systems Department.

Within each of these areas, specific risk situations were identified:

A. Technological Infrastructures:
    - Procedures for recovering information and operations in the event of a disaster; and
B. Communications:
    - Vulnerabilities of websites to intrusions that jeopardize their availability or the confidentiality/integrity of information.

Regarding each of these risk situations, the prevention measures adopted/to be implemented were specifically identified, namely:

A. Technological Infrastructures:
    - Information and operations disaster recovery procedures:
        i. Disaster Recovery Plan;
        ii. Business Continuity Plan;
        iii. Business Continuity Policy;
        iv. Business Continuity Objectives; and
        v. Backups Policy.
B. Communications:
    - Vulnerability of websites to hacking which compromises their availability or the confidentiality/integrity of information:
        i. Analysis supported by the Bitsight – Cyber Security Rate tool; and
        ii. Rapid 7 – insightIDR.

All preventive measures were already in place, only the Rapid 7 – insight IDR tool was pending implementation, which was scheduled to be implemented in Q4 2022.

This technological tool was, however, replaced by another tool – QRadar – S21SEC – which, in accordance with the state of the art, the Information Systems Department believed to provide greater technological robustness in terms of security[4], which was fully implemented during Q4 of 2022.

It should be noted that the other measures continue to be successfully implemented (considering that these are measures aimed at preventing the risks specifically identified therein), and there have been no incidents that justify the review of the preventive measures listed therein.

[4] This tool is able to optimize the capabilities of detection, analysis, prioritization and investigation of security threats, providing a unified visibility of the indicators of all environments (*On-prem* and *Cloud*).

Following the adoption of the aforementioned measures, the two areas in which there were high-risk situations saw a reduction in risk to a moderate level, and there are no longer any high- or critical-risk situations at Novabase.

3. Interim Assessment

Overall, we consider that the preventive measures adopted are suitable and adequate to prevent the risks identified in the Plan for the Prevention of Risks of Corruption and Related Offences (without prejudice, naturally, to being continuously reviewed and updated in accordance with the best practices in the industry, in fulfilment with a practice of continuous improvement).

4. Publicising

This Report will be duly publicised internally and externally, as required by Law.

5. Annexes

This Report comprises the following Annex (numbering corresponding to the numbering given in the Plan for the Prevention of Risks of Corruption and Related Infractions):

5.1. Annex II: Risks and Prevention Measures (Reassessment of High-Risk Situations)

NOVABASE

Annex II

Risks and Prevention Measures

(Reassessment of High-Risk situations)

Situations of risk	Impact	Likelihood	Risk level	Prevention measures	Implementation deadline	Area in charge
	Technology Infrastructures					
Information and operations disaster recovery procedures	High	Low	Moderate	Disaster Recovery Plan	Implemented/ on going	Information Systems Department
				Business Continuity Plan		
				Business Continuity Policy		
				Business Continuity Goals		
				Backup Policy		
	Communications					
Vulnerability of websites to hacking which compromises their availability or the confidentiality/integrity of information	High	Moderate	Moderate	Analysis supported by the BitSight – Cyber Security Rate tool	Implemented/ on going	Information Systems Department
		Moderate		QRadar – S21SEC	Implemented/ on going	Information Systems Department

NOVABASE