

Risk Control and Management Policy

Prosegur Compañía de Seguridad S.A.
29/07/2020



Table of contents

1. Purpose
2. Scope
3. Roles and Responsibilities
4. Basic Principles
5. Risk Map
6. Risk factors
7. Approval and Dissemination



1. Purpose

The purpose of this Risk Control and Management Policy is to establish the basic principles and overall framework for action for the control and management of risks faced by Prosegur Compañía de Seguridad S.A. (hereinafter “Prosegur”) and the other subsidiary companies that make up the Prosegur Group. It also defines the risk control and management model, the types of risk, the level of risk deemed acceptable, the measures to mitigate the impact of risks, the control and information systems used to control and manage risks, the definition of competencies, functions and responsibilities of the positions involved in the risk management process and where, within the corporate governance structure, does the responsibility for risk supervision lie.

2. Scope

The Risk Control and Management Policy shall be applied by all the companies that make up Prosegur, that is, all the companies over which Prosegur Compañía de Seguridad S.A. has effective control. Prosegur Cash S.A. and its subsidiaries may establish their own risk control and management policy, respecting the principles laid down in this policy.

The Risk Control and Management Policy shall be applied, as a framework policy, by all the businesses and support areas of Prosegur. The risk control and management model shall cover all types of risks that may jeopardise the achievement of Prosegur’s objectives. By means of this policy, Prosegur undertakes to develop all its capacities so that all types of risks are adequately identified, measured, prioritized, managed, supervised, controlled and mitigated.

3. Roles and Responsibilities

All of the persons that make up Prosegur have some responsibility in risk control and management.

Supervision of the risk control and management system

In addition to the general function of supervision, the **Board of Directors of Prosegur** is ultimately responsible for determining the general risk management and control policies and strategies of Prosegur, delegating to the **Audit Committee** the power to inform, advise and propose in relation to these policies and strategies and to monitor the functioning of the risk management and control unit, through Prosegur's Internal Audit Department.

The **Risk Committee**, as risk control and management unit of Prosegur, ensures the proper functioning of the risk control and management systems and, in particular, that all significant risks affecting Prosegur are properly identified, managed and quantified; participates actively in drawing up the risk strategy and in important decisions on risk management; and ensures that the risk control and management systems adequately mitigate risks.

Persons responsible for managing risks

The Heads of Prosegur's Businesses and Support units shall own each of the identified risks and actively participate in the assessment of those risks, their effective control and mitigation, the level of risk deemed acceptable, and any decision affecting risk management. To this end, each identified risk shall be assigned to a risk manager who shall have total competence over all matters regarding the control and management of the risk, who shall establish the effective control mechanisms and, where appropriate, draw up a mitigation plan, and who shall effectively monitor the evolution of the risk.

In this regard, all staff shall be aware that the information provided regarding risk control and management shall meet the following requirements:

- ◆ The information is complete, ensuring that all the information that is relevant for adequately controlling and managing risks is disclosed.
- ◆ The information is true and accurate, making sure that the information disclosed contains no errors.
- ◆ The information creates value, by promoting the development of a risk control and management culture.
- ◆ The information is provided in a timely manner, i.e. as soon as it is known and is relevant for an adequate control and management of risks.

Internal Audit

Prosegur's Internal Audit Department shall provide objective assurance to Prosegur's governing bodies regarding the effectiveness of the risk control and management activities of Prosegur, helping to ensure that key business risks are being properly managed and that the risk management and control system is working effectively.

It shall fulfil the following requirements:

- ◆ Provide assurance regarding risk control and management processes.
- ◆ Provide assurance that the risks are correctly assessed.
- ◆ Evaluate the control and risk management processes.
- ◆ Assess the reporting of key risks.
- ◆ Review the control and management of key risks.

4. Basic Principles

Prosegur is subject to various risks inherent to the different countries and markets in which it operates, and to the activities it carries out, which can undermine, and even prevent it from achieving its goals and executing its strategies successfully.

Prosegur carries out control activities by means of the appropriate policies and procedures to help prevent and detect the materialisation of risks and, if they do materialise, mitigate, compensate or correct their impact. In this way, the aim is to ensure that the risks assumed by Prosegur are compatible with its objectives in the short and medium term.

Prosegur has an adequate control and management of risks system in place and assumes a controlled level of risk in order to:

- ◆ Achieve the strategic objectives approved.
- ◆ Provide the maximum level of guarantees to shareholders.

- ◆ Defend the interests of shareholders, customers and other stakeholders concerned with the development of Prosegur.
- ◆ Protect its results and its reputation.
- ◆ Ensure sustained financial stability and soundness.

The risk control and management system is based on procedures and methodologies that allow risks to be identified and assessed in order to achieve these objectives.

Risk assessment is carried out according to pre-established tolerance levels, so that the assessment forms the basis for determining how risk management will be carried out.

The actions aimed at controlling and mitigating risks are summarised below:

- ◆ Ensure sustained financial stability and soundness.
- ◆ Identification, prioritisation, and evaluation of critical risks on an ongoing basis, considering their possible impact on Prosegur's strategic objectives.
- ◆ Risk assessment according to procedures based on key indicators that allow risk control, risk management evaluation and monitoring the evolution of risks over time.
- ◆ Periodic monitoring of the effectiveness of the measures applied by those responsible for managing risks to prevent and mitigate the effects of the materialisation of any of the risks.
- ◆ Review and analysis of results by Prosegur's Risk Committee.
- ◆ Supervision of the system by the Audit Committee, through the Internal Audit Department.

5. Risk Map

The Risk Map is the management and information tool through which Prosegur's risks are controlled and managed that graphically displays the diagnosis of the risk assessment process. It is determined through the interaction of the probability and impact of the risks on the different processes, activities and functions of a business or support area. It is a helpful tool for the review of the internal control in place to mitigate risk impact.

The risks included in the map are assessed qualitatively, in order to establish their probability of occurrence, and are also assigned a quantitative indicator, in terms of impact level.

Each person responsible for managing risks continuously evaluates each of the identified risks, establishes the effective control measures that are to be taken and proposes the implementation of corrective or mitigation measures.

Prosegur's Internal Audit Department promotes and coordinates the model by drawing up the risk map, along with corporate and country managers, and through the follow-up information submitted to the Risk Committee.

The Audit Committee shall review Prosegur's risk map as often as considered necessary to ensure an adequate monitoring of risks, with the support of the Internal Audit Department. The updating of the risk map, both at corporate level and in each of the businesses, shall be carried out by each of the persons responsible for managing the risks.

6. Risk Factors

The risk factors to which Prosegur is subject are, in general, the following:

Operational and business risks.

Prosegur's operations are carried out in sectors and markets that, in some cases, may be undergoing concentration processes or facing other adverse situations that may significantly affect Prosegur's turnover. The impact of the unfavourable economic environment, the concentration of the financial sector and the situation of the public sector is reflected in a contraction of demand, in particular, on the European markets. Likewise, operations may be affected by the economic downturn.

If, due to adverse market conditions, such as concentration processes in the financial sector or prolonged decrease in the use of cash (which would mainly affect the transport of valuables and cash management business), a reduction in demand for security services by the public sector or cost containment policies applied by private companies (which would mainly affect the manned guarding business), or a reduction of activity in the construction sector and a downturn of the real estate market (which would mainly affect the technology and alarm businesses), there is a substantial contraction in the demand for services or facilities, Prosegur might not be able to achieve its planned turnover, which would affect its results.

On the other hand, Prosegur's operations are carried out in highly competitive sectors and markets with price pressures. In particular, manned guarding markets are highly fragmented and have relatively low entry barriers. Although Prosegur does not compete only on price, due to the difference in services provided with regard to its competitors and broad brand-name recognition, actions taken by competitors, especially aggressive pricing policies, can exert considerable pressure and affect Prosegur's prices, margins and results.

There is also the possibility that a counterparty of Prosegur, especially customers, may fail to discharge its contractual obligations and cause a financial loss for Prosegur affecting its results.

Financial, interest rate, exchange rate and tax risks

Prosegur's earnings and equity may be affected by unforeseen changes in interest rates or exchange rates.

Prosegur is exposed to interest rate risk due to the monetary assets and liabilities recognized on its balance sheet. It is also exposed to exchange rate risks arising from income generated in different currencies, as the reference currency is the euro. Exchange rate fluctuations also affect the company's financing costs for instruments denominated in currencies other than the euro.

Finally, an inadequate analysis or interpretation of the tax rules could lead to delays in the recovery of deferred taxes, a higher tax burden and even penalties.

Technological Risks

The activities carried out by Prosegur and the other companies of the Prosegur Group, especially those linked to the transport of valuables and cash management services and connections to alarm reception centres, are highly dependent on its information technology infrastructure and communications. Significant problems with the infrastructure, such as inadequacy or disruption of telephone and technology systems, prolonged disruption of applications, or intrusion into information systems could halt or delay the provision of the service to customers, hinder the ability to manage businesses and may result in significant costs being incurred.

In the normal course of business, Prosegur collects, manages, processes, and stores sensitive and confidential information, including business and operational information relating to its customers and personal information of customers and employees.

Despite the security measures in place in facilities and IT systems, information held by Prosegur could be vulnerable to security breaches, computer viruses, data loss, human error, or other similar events.

Any breach of security through misappropriation, loss or other unauthorized disclosure of confidential information by persons connected to Prosegur or by third parties outside the company, could cause significant damage to Prosegur's reputation, result in litigation and have a material adverse effect on Prosegur's results of operations.

Legal, social and regulatory risks.

Prosegur's operations are subject to various regulations in the countries in which it operates that usually require authorisation for the provision of security services. Prosegur's activity is mainly subject to regulations governing private security, labour and social security regulations, tax regulations, arms control regulations, laws and regulations on capital markets and regulations on the prevention of money laundering, competition regulations and data protection regulations.

Prosegur's operations and the structure of the businesses include procedures to ensure compliance with laws in all of the countries in which it operates, although failure to comply with laws could result in fines, limitations on activity or revocation of authorisation to operate.

Changes in regulation may require changes in operational models which, in turn, may involve additional costs. Prosegur's results may also be affected by unfavourable changes in regulatory conditions, such as labour and tax legislation or restrictions for obtaining permits and licences.

Reputational Risks

The success over time of Prosegur's businesses is largely based on the trust that comes from the quality and control of the services it provides, its reputation as a company and the integrity of its employees.

The reputation of Prosegur and its brand and, in particular, the trust bestowed upon the company by its customers, could be seriously damaged by real or perceived incidents that affect the ability to carry out its operations in an ethical, responsible and safe manner. Likewise, Prosegur's reputation may be damaged if it fails to meet the expectations of key stakeholders.

Environmental risks.

Environmental risks are those referring to direct or indirect economic losses caused by external events, some of which associated with climate change. Non-compliance with environmental regulations could lead to sanctions or a negative perception by Prosegur's customers.

Political risks.

Prosegur operates in several countries, the political risk is that which affects the economic interests of the company, as a consequence of changes or lack of political stability in a country or region.

The various repercussions it may have range from increase in operating costs, to commercial and economic losses or even the closure of our activities.

Risks of Corruption and fraud.

Prosegur carries out its activities through various operating companies located in different countries, which may be affected by cases of corruption and/or fraud. These risks may affect the economic development of these countries and even jeopardise their state and governance model, undermine the principles of equality and competition in the markets and cause serious damage to social order, political stability, and the economy.

Although Prosegur has a strong crime prevention programme in the countries in which it operates implemented through policies, procedures and the establishment of controls to prevent corruption, fraud and any other illegal activities in which an employee, director, shareholder, customer or supplier or any related third party acts dishonestly, the materialisation of these risks can affect the company's reputation and financial situation.

7.- Approval and Dissemination

This Risk Control and Management Policy was approved by the Board of Directors on 29 July 2020, following a favourable report from the Audit Committee, and shall be in force as from this date.

The Heads of the businesses and support areas shall take the necessary measures to ensure dissemination, training and compliance with this policy.