

2.2. Risk management

The Prosegur Risk Management System allows the company to implement proactive risk management, identifying the most critical aspects, evaluating the same and supervising their management via key risk indicators. The system is also based on the COSO (Committee of Sponsoring Organizations of the Treadway Commission) standard, supported by other standards such as Basel III in the financial sector and ISO 31000. Furthermore, it operates comprehensively and continuously, consolidating management by area, business unit, activity, subsidiary, geographical area and support area at the corporate level.

Depending on the risk type and relevance, Prosegur management and direct supervisors establish specific procedures to ensure anticipation, with early detection and prevention measures in order to prevent risks from materialising, as well as developing mitigation strategies. The Board of Directors, the most senior body responsible for risk control and management policy, supervises internal information and control systems. The results of risk management and control are periodically reviewed and analysed by the **Corporate Risk Committee**.

Risk management cycle



Thus, the Prosegur Risk Policy includes the core principles that are central to risk management and control:

- › Identification, assessment and prioritisation of critical risks.
- › Risk assessment in accordance with procedures based on key indicators, to support risk control and appraisal.
- › Regular monitoring of assessment results and the efficacy of the applied measures.
- › Review and analysis of results by the Risk Committee.
- › System supervision by the Audit Committee.



RISK FACTORS	RISK	MITIGATION STRATEGY
REGULATIONS on private security, workplace and social security regulations, tax regulations, regulations on arms control, regulations on capital markets and antimoney laundering regulations	Greater intervention by governments and regulators	<ul style="list-style-type: none"> › Business diversification in differentiated markets
	Risk of non-compliance with applicable laws	<ul style="list-style-type: none"> › Corporate Compliance Programme › Independent processes of due diligence
BUSINESS RISKS: Decrease in the demand; prolonged reduction of cash use, highly competitive markets, aggressive pricing policies, relatively low entry barriers	Circumstantial reduction in the demand for security services	<ul style="list-style-type: none"> › Business diversification in differentiated markets
	Operations in highly competitive markets	<ul style="list-style-type: none"> › Development of new value added products and services that differentiate Prosegur from the competition
	Not reaching forecasted results in alarms	<ul style="list-style-type: none"> › Increase Prosegur's brand recognition
	Inadequate management of indirect costs	<ul style="list-style-type: none"> › Operational efficiency measures
REPUTATIONS: Real or perceived incidents that affect its ability to operate in an ethical, responsible and safe fashion	Negative publicity about Prosegur	<ul style="list-style-type: none"> › Detect potential irregularities through the Whistleblowing Channel › Prevent non-compliance by means of the Corporate Compliance Programme › Independent due diligence processes

RISK FACTORS	RISK	MITIGATION STRATEGY
<p>OPERATIONAL AND TECHNOLOGIACAL RISKS: Interruption or failure of communications, unauthorized access to information systems, security breaches, data loss, operative errors, incidents involving assets or lost cash.</p>	<p>Loss or theft of proprietary information or confidential information of customers</p>	<ul style="list-style-type: none"> > Global logical security policies
	<p>Failures or incidents in IT infrastructure</p>	<ul style="list-style-type: none"> > Monitoring the processes of controlling and monitoring traceability of the transport, handling and storage of cash operations
	<p>Incidents involving assets under custody or lost cash</p>	<ul style="list-style-type: none"> > Independent assistance in claims or differences arising in the cash management activity > Identification of best practices > Drawing up policies on physical security and procedures that minimize potential losses > Implementation of business continuity policies and recovery plans > High quality and reliable insurance coverage
<p>FINANCIAL RISKS: Interest rate risk, exchange rate risk, counterparty and fiscal risks.</p>	<p>Cash generation or cash management</p>	<ul style="list-style-type: none"> > Dynamic analysis of interest rate risk exposure > Simulation of several scenarios depending on refinancing, renewal of present positions, alternative financing and coverage > Calculation of the effect of a certain change in the interest rate on the result > Natural hedging policy > Customer risk assessment > Monitor, on a monthly basis, the credit status of customers and application of valuation adjustments > Perform transactions with entities with defined credit ratings. Signing of financial transactions framework agreements (CMOF or ISDA) > Define counterparty risk limits > Regular publication of updated credit limits and levels



2.2.1. Operating risk management

Prosegur works hard to manage and control operational and regulatory compliance risks, as these may potentially have a bearing on its commitments with stakeholders, especially clients and employees. Prosegur adopts an approach to risk management that encompasses all areas of activity at the company, via strict controls based on three priority action areas: Infrastructure, processes and people.


The company has set up a Global Risk Management Division to secure optimal risk management

efficiency. Thanks to its exceptional structure and organisation, this division affords the company a competitive edge over its peers when it comes to risk management.

The Division has all the instruments it needs to efficiently manage risks associated with operational security. It also provides the required tools to maintain and uphold the standards and procedures defined by the company, while ensuring compliance with applicable law and national regulations.


With central offices in Madrid (Spain), the Division is comprised of three departments, which are represented both regionally and nationally: Security, Intervention and Insurance. The integration of these three departments into a single Division ensures optimal operational efficiency at the lowest possible cost, thanks to in-house specialists sharing common procedures.

 **The Security department** oversees risks and legal regulations in the field of security and acts as the organisation's second line of defence, taking an active role in the development and implementation of security business operations. The department has employees distributed across four global support areas: Intelligence, Information Security, Security of Bases and Facilities, and International Tactical Training Team.

 **The Insurance department** identifies and controls operating risks and establishes the fundamentals for assurance and management, minimising any impact on financial statements. The department sets up insurance programmes, signing policies at the corporate and local levels with leading insurance companies to provide coverage for an extensive range of risks: employee risks, direct and indirect risks arising from Prosegur's activity and risks affecting

items of property, plant and equipment. In 2018 the Insurance department added coverage for cybernetic risks, extended the geographic coverage for credit insurance to Chile and Colombia, while also extending professional civil liability coverage to the entire organisation.


Global Risk Management Division

 **Security department**


SUPPORT AREA

- > Security at operational sites and facilities
- > International Tactical Training Team
- > Intelligence
- > Information Security

Countries

 **Intervention department**

- > Europe and Asia Pacific
- > Latin America
- > Brazil

 **Insurance department**

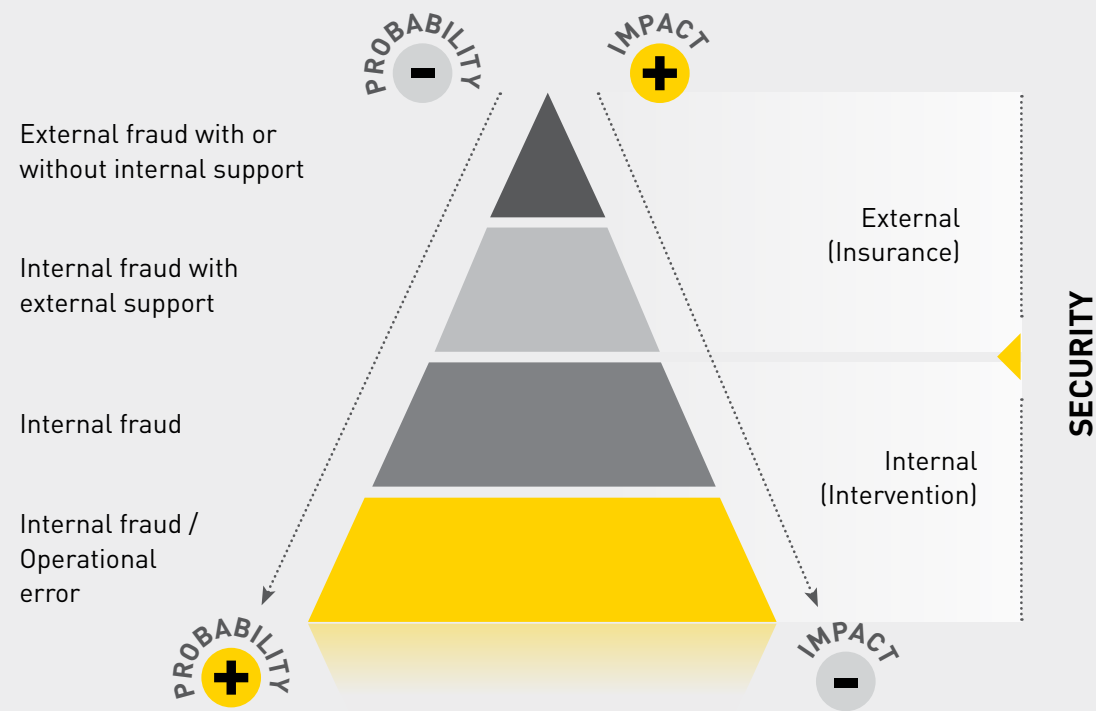
- > Operational Structure

Countries



Risk Approach

Security model based on risk management and strict control of infrastructures, processes and people.



Milestones in 2018

Security

Efforts were made during 2018 to enhance protection at operational sites, strengthen Remote Control Centres and modernise tracking equipment for armoured units.

Intervention

During 2018 the Intervention department conducted 325 operational reviews and 334 vault audits in the Prosegur Cash business; 73 operational reviews in the Prosegur Security business; end-to-end business reviews for Prosegur Alarms in 8 countries; and 11 transversal audits for support processes across all businesses.

A risk management and control model was implemented during the period for the Prosegur Alarms business, encompassing Spain, Portugal and Latin America. The model draws significantly on support from data analytics tools, helping to provide comprehensive continuous monitoring

and more efficient use of resources. In turn, a risk model was established in the Prosegur Security business for services that are susceptible to major impacts when a negative event occurs, seeking to identify risk exposure situations that might require improved operational implementation or a review of service provision conditions.

During 2018 the Loss Control Unit launched a new application intended to provide daily control over vault closures. The deployment began in Brazil and is set to be rolled out to the remaining countries in 2019. This application features improved functionalities and capabilities compared to its predecessor.

Insurance

In 2018 the Insurance department added coverage for cybernetic risks, extended the geographic coverage for credit insurance to Chile and Colombia, while also extending professional civil liability coverage to the entire organisation.

