

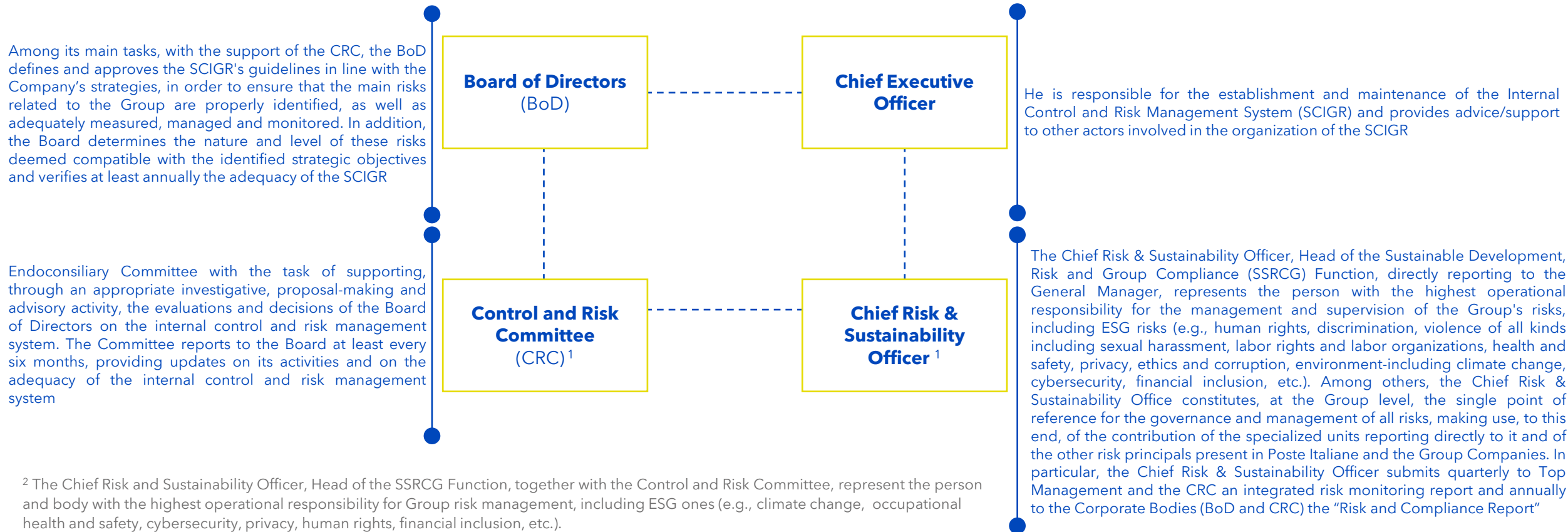
POSTE ITALIANE

Risk Management | Insights

Risk Governance

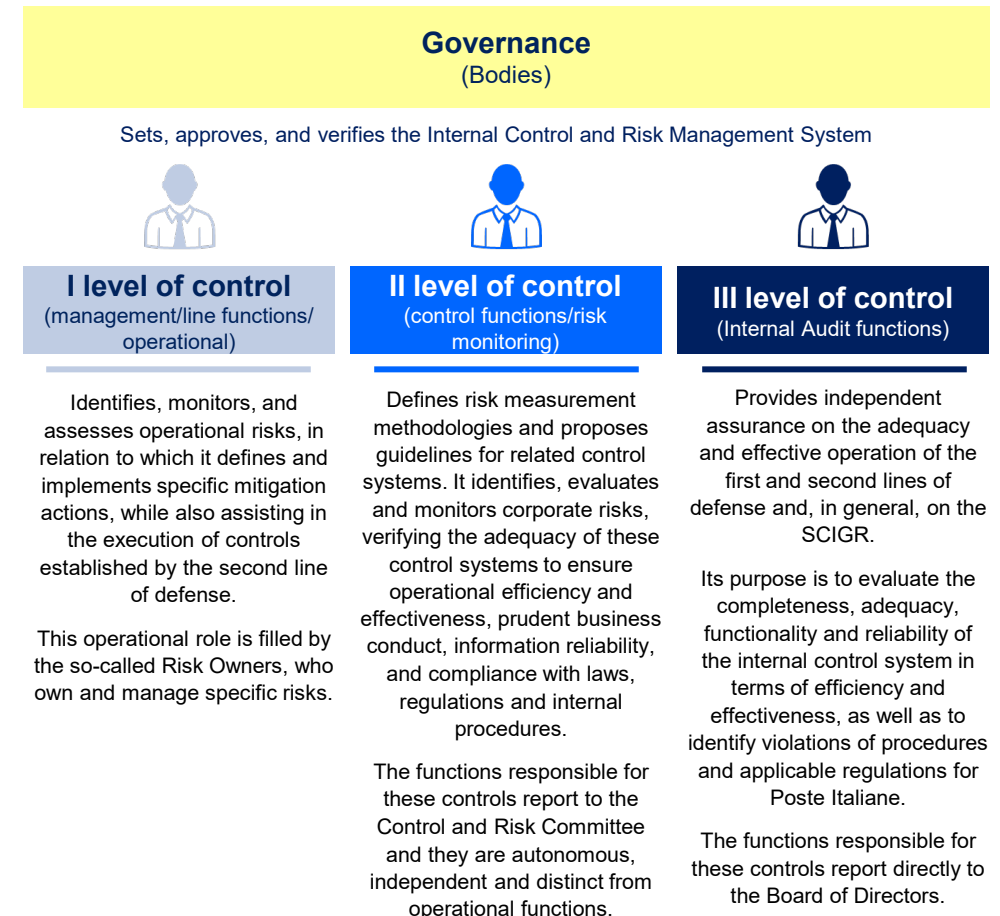
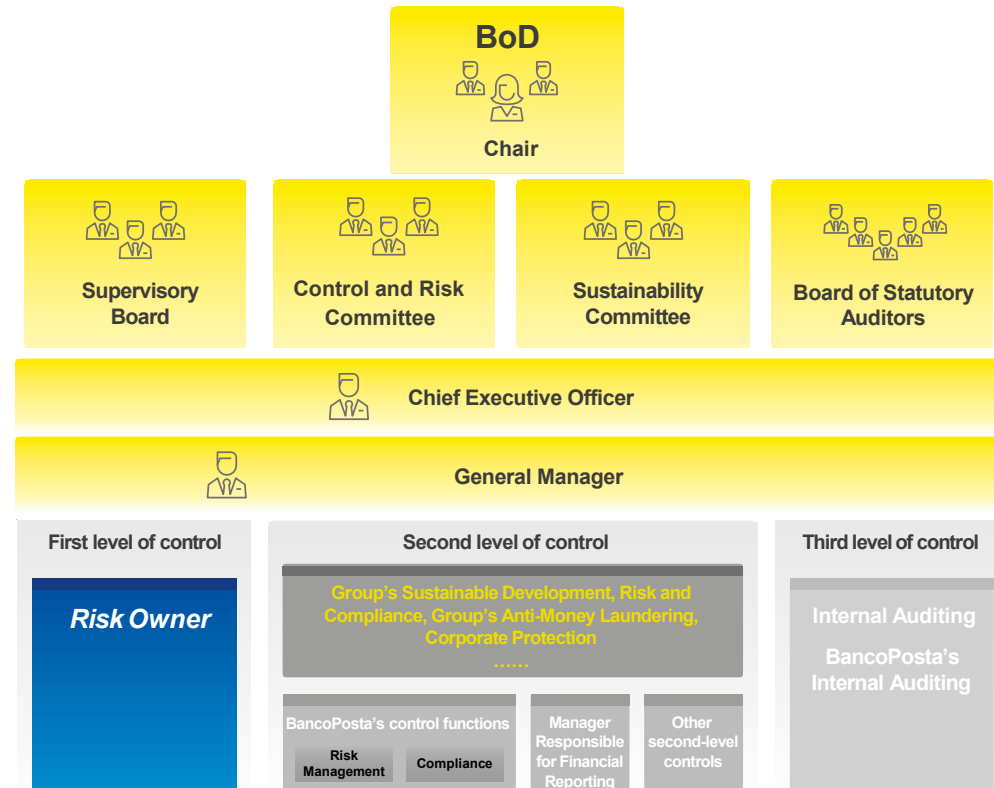
GROUP RISK GOVERNANCE

In order to ensure an adequate and effective identification and management of Group risks, Poste Italiane has defined a specific governance in the area of risks, which is represented below:



FOCUS RISK GOVERNANCE FRAMEWORK | THE THREE LINES OF DEFENSE MODEL

Poste Italiane Group has defined, in order to ensure appropriate management of corporate risks, a Risk Management governance framework structured according to the Three Lines of Defense Model (COSO Framework), summarized below. For further details, please refer to the Guidelines on the Group's Internal Control and Risk Management System (SCIGR).



Risk Review | Focus

RISK CATEGORIES IDENTIFIED BY THE GROUP

Below are the main risk categories associated with the Poste Italiane Group's activities, as identified in the Group's Risk Model¹.

CATEGORY	STRATEGIC	OPERATIONAL	COMPLIANCE	REPUTATIONAL	ESG	FINANCIAL AND INSURANCE
DESCRIPTION	Risks that could influence achievement of the goals set out in the Strategic Plan	Risks of incurring losses resulting from inadequate or failed internal processes, people and systems at Group level, or from external events	Risks of breaches of existing laws and regulations or related to the introduction of new legislation or regulations of either general importance or specific to the sectors in which the Poste Italiane Group operates	Risks connected with a negative perception among the Group's stakeholders, in response to which the Group has adopted a stakeholder engagement framework in order to identify and assess this type of risk at source	Risks arising from factors related to environmental, social and governance issues (in particular, linked to human rights, climate change and sustainable finance)	Financial risks that are regulated and overseen by supervisory authorities (Bank of Italy and IVASS) and the responsibility of the Risk Management units belonging to the various business units, coordinated by the function responsible for Sustainable Development, Risk and Compliance

¹ The Group evaluates its risk exposure on a quarterly basis.

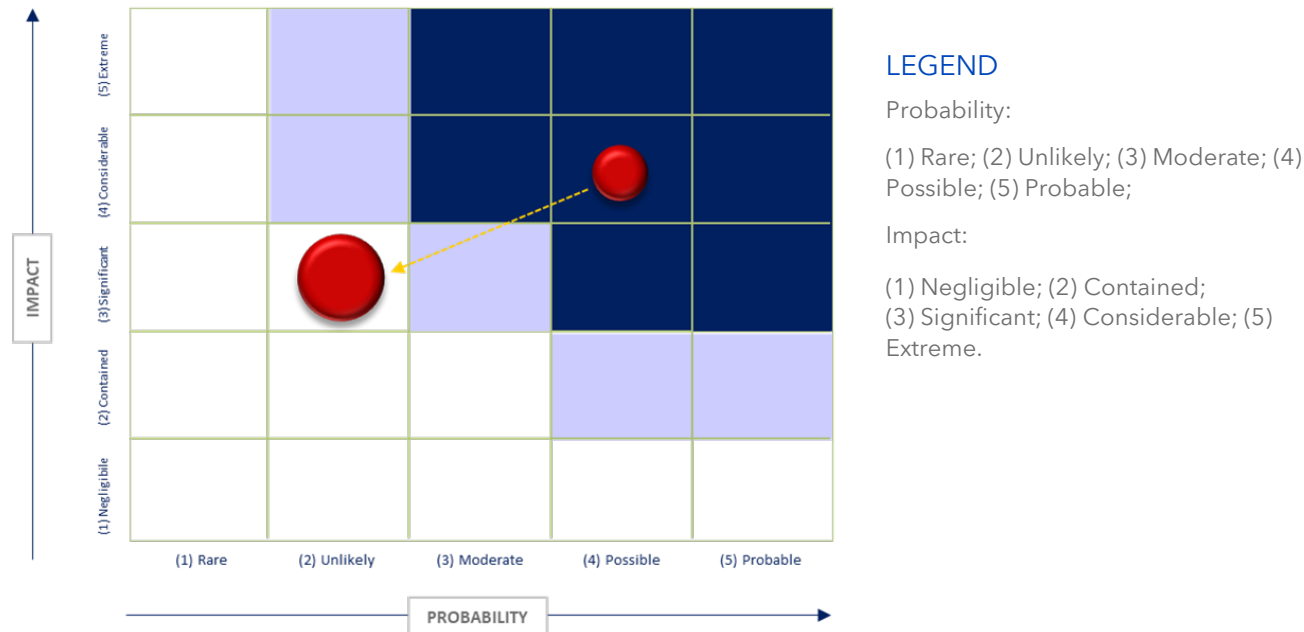
The "Internal Auditing" function annually internally audits the Group's System of Internal Control and Risk Management (SCIGR), preparing an Evaluation Report on the same System which is, subsequently, approved by the Board. The purpose of the Report is to express an overall assessment of the SCIGR in "Positive Assurance" mode. In addition, the compliance of Poste Italiane's Risk Management System is also verified annually through external audits conducted by third-party entities as part of the verification activities of the ISO 37301 certification and recertification processes, and as part of the additional verification activities implemented to maintain/obtain the numerous ISO certifications achieved by the Group.

RISK ASSESSMENT

For each identified risk, the Group determines the level of risk in two perspectives:

- the **Inherent Risk** profile, determined by considering the risk component intrinsic to the very nature of the specific Activity, without taking into account the existence and effective operation of the risk treatment actions in place;
- the **Residual Risk** profile, determined by considering the level of intensity of treatment actions¹.

The overall residual risk assessment allows the prioritization of risks and is represented within a heatmap (probability-impact matrix), as illustrated below as an illustrative example:



Depending on the placement on this matrix, risks can be classified according to the following areas of relevance:

- Tier 1 (dark blue area);
- Tier 2 (light blue area);
- Tier 3 (white area).

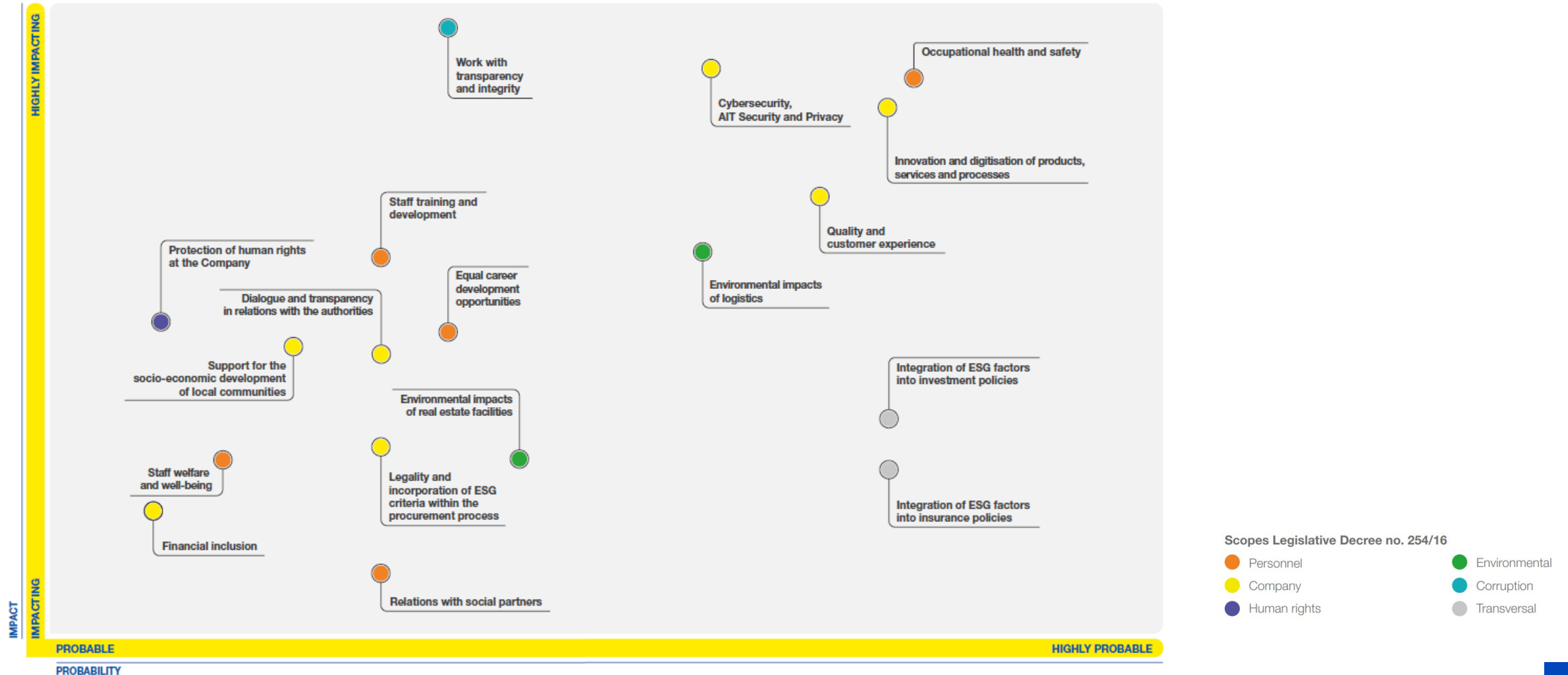
Risks that belong to "Tier 1" and "Tier 2" are called "Top risks".

¹ The level of intensity of the treatment actions to be deployed is also assessed by taking into consideration the conduct of scenario analysis (stress tests), both on certain types of financial risks and non-financial risks (e.g., risks related to climate change, anti-corruption issues, cybersecurity risks, etc.).

FOCUS | POSTE ITALIANE GROUP'S RISK MATRIX

Company-specific risk exposure

Below is the Poste Italiane Group's matrix illustrating the company-specific risk exposure, considering the probability and magnitude associated with each risk.



EXAMPLES OF MITIGATION ACTIONS AND CORPORATE RISK CULTURE

EXAMPLES OF MITIGATION ACTIONS

CYBERSECURITY, IT SECURITY AND PRIVACY	<p>Poste Italiane Group, in order to mitigate risks related to cybersecurity and privacy, has adopted appropriate risk assessment processes and precautionary measures. Below are the main mitigation actions implemented:</p> <ul style="list-style-type: none"> • technical security audits carried out on the three applications: Vulnerability Assessment, Static and Dynamic Code Review, Penetration Test • obtain/maintain ISO 27001 and 20001 certifications • definition and implementation of a business continuity plan which identify the most critical systems, the potential threats that may occur on them and the countermeasures to be adopted • adoption of the Framework Privacy that ensuring compliance with the monitoring obligations of the main business processes • introduction of the Privacy Policy followed by audits that ensure compliance with the same
ENVIRONMENTAL IMPACTS OF REAL ESTATE FACILITIES	<p>The Poste Italiane Group, in order to mitigate risks related to the environmental impacts of its properties, has adopted appropriate risk assessment processes and precautionary measures. Below are the main mitigation actions implemented:</p> <ul style="list-style-type: none"> • use of electricity from renewable sources (99% of the electricity purchased by the Group comes from 100% renewable sources, certified by Guarantees of Origin) • adoption of the Environmental Management System certified ISO 14001 • construction of 1,400 photovoltaic systems by 2026 with the aim to cover 15% of the Company's energy needs • continuation of the Smart Building Project with the aim to create a management system in terms of Building and Energy Management System (BEMS) • launching the decarbonisation project aimed at replacing gas boilers with heat pumps on about 100 sites • use of smart technologies, installing LED technology lighting systems

CORPORATE RISK CULTURE

- In order to ensure adequate dissemination of the risk management principles adopted within the Company, the Poste Italiane Group has launched a number of specific initiatives, such as:
- vertical training initiatives on risk management principles for the corporate population, such as those related to ESG risk management principles identified as relevant to Poste Italiane Group. The efforts of the SSRCG function include the delivery of specific training courses on risk management and regulatory compliance. In fact, in 2023, the Group provided about 6.5 million hours of training, including courses useful for promoting an effective risk culture. By way of example but not limited to, in order to promote awareness of corruption and health and safety issues, the Company provides mandatory ongoing training through both e-learning and classroom courses on these topics;
 - periodic training of the Board of Directors on corporate risks, the initiatives undertaken in this regard for their mitigation and with respect to monitoring activities;
 - relevant functions engage with risk management function for the preliminary assessment of risks deriving from the definition of the new product, for evaluating the financial sustainability associated with the initiative being developed, and for the definition of a business case in order to ensure that the risks deriving from the development of the new product / service are consistent with the Company's propensity to risk;
 - integration within the financial incentive systems (MBO and LTI) of metrics related to the Group's risk management, such as those related to sustainability aspects considered as relevant (e.g., green transition, ESG Strategic Projects, MPD quality, people development, etc.). These are integrated with the aim of further enhancing the management of risks related to these issues. In addition, Poste Italiane Group also takes into account the risk-adjusted profitability parameter used by BancoPosta.

FOCUS | RISK APPETITE FRAMEWORK

Objectives

Based on the Corporate Governance Code, the Board of Directors, after consultation with the Control and Risk Committee, defines the nature and level of risk compatible with the strategic objectives, taking into account the various risk factors including exogenous ones (e.g., the evolution of the macroeconomic environment).

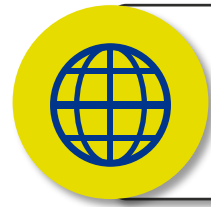
Risk Appetite Framework - Objectives



Ensure that the **Group's business**, as articulated in entities, **develops within the acceptable and tolerable risk** levels established by the Board of Directors



Ensure the **sustainability of strategic objectives with respect to the assumed risk profile** against the different types of risks



Declining the Group's sustainable risk profile with reference to the following year while meeting stakeholder expectations and/or applicable regulatory requirements



Coordinate and integrate the safeguards of supervised entities that define their own **individual RAFs** approved by their respective Boards of Directors

At the Group level, following the strategic risk assessment process, a set of indicators, with respective thresholds, is included alongside the indicators relating to the top risks identified, relating to risks whose performance is mainly influenced by the **evolution of the macroeconomic environment**. Moreover, these indicators also summarize the most relevant financial and insurance risks for the Poste Italiane Group.

Group Indicators are subject to **BoD approval** and quarterly monitoring, the outcomes of which are represented to the CRC. Regarding **Dividend, Liquidity** and **Financial Structure, Economic Performance** indicators, the relevant thresholds are also submitted to the BoD for approval.

In determining these thresholds, budget forecasts are incorporated and protection limits are identified, when they are exceeded, there is a reporting to the relevant Corporate Bodies and, at the level of individual Group entities, an escalation process aimed at identifying and evaluating any corrective managerial actions to restore the original trajectory.

FOCUS | RISK APPETITE FRAMEWORK

Risk Appetite Framework Process

In order to further strengthen the degree of integration with individual RAFs, both in terms of indicators and the criteria for defining the respective thresholds, the continuous path of integration in risk management sees coordination between all Risk Management structures operating within the Poste Italiane Group. In particular, the Group RAF is also shared with the Risk Managers of the individual supervised entities:

Risk Appetite Framework Process

