## 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:

Among its main tasks, with the support of the CRC, the BoD defines and approves the SCIGR's guidelines in line with the Company's strategies, in order to ensure that the main risks related to the Group are properly identified, as well as adequately measured, managed and monitored. In addition, the Board determines the nature and level of these risks deemed compatible with the identified strategic objectives and verifies at least annually the adequacy of the SCIGR

Endoconsiliary Committee with the task of supporting, through an appropriate investigative, proposal-making and advisory activity, the evaluations and decisions of the Board of Directors on the internal control and risk management system. The Committee reports to the Board at least every six months, providing updates on its activities and on the adequacy of the internal control and risk management system

**Chief Executive Board of Directors Officer and General** (BoD)<sup>1</sup> Manager **Head of Corporate Control and Risk** Affairs / Committee Co-General (CRC) Manager<sup>2</sup> **Sustainable Development, Risk** and Group **Compliance** 

(SDRC)

Is responsible for the establishment and maintenance of the Internal Control and Risk Management System (SCIGR) and provides advice/support to other actors involved in the organization of the SCIGR

Ensures the unitary governance of issues related to the internal control and risk management system, supporting Top Management in the effective implementation and management of Risk Management and Integrated Compliance processes at Group level, with reference to all types of risk. In particular, the Co-General Manager presents on a quarterly basis integrated risk monitoring reports to senior management and the CRC and annually the "Risk and Compliance Report" to Corporate Bodies (BoD e CRC)

Established within the Corporate Affairs structure, it represents the single point of reference for the governance and management of all risks from a Group perspective. The SDRC function, which reports to the Company's Co-General Manager, defines, for each area of risk, standard policies, tools and methodologies in order to ensure an integrated and comprehensive approach at the Group level

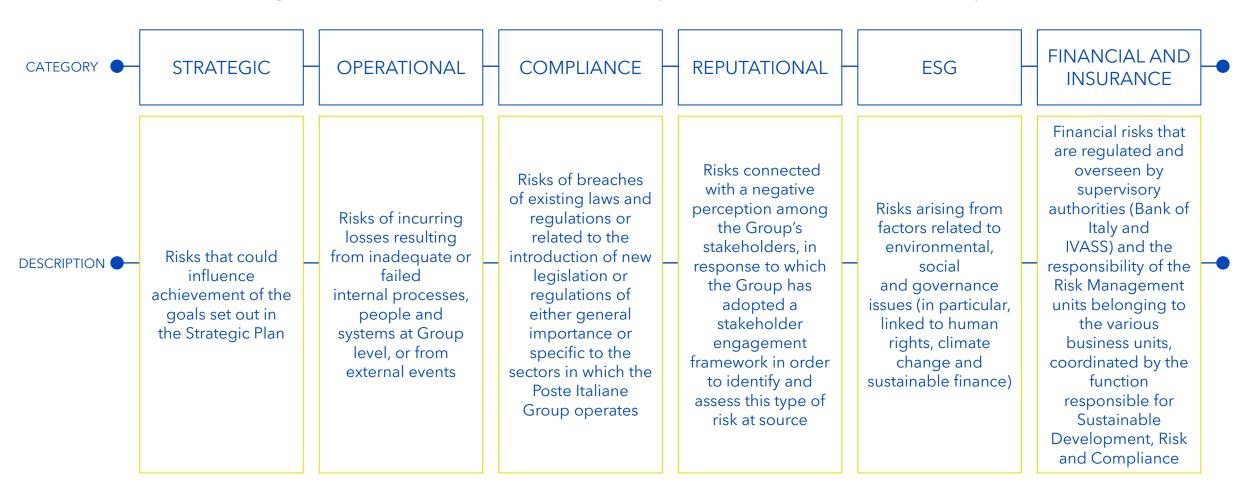
<sup>&</sup>lt;sup>1</sup> The BoD is periodically informed and trained with respect to risk management issues (e.g., through induction training initiatives).

<sup>&</sup>lt;sup>2</sup> The Head of Corporate Affairs / Co-General Manager of the Group operates as the Chief Risk Officer; together with the Control and Risk Committee they represent the person and body with the highest operational responsibility for Group risk management, including ESG ones (e.g., climate change, occupational health and safety, cybersecurity, privacy, human rights, financial inclusion, etc.).

# 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 Model<sup>1</sup>.



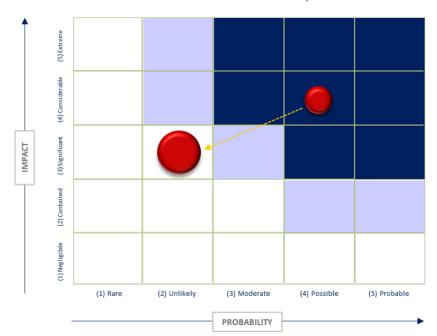
<sup>&</sup>lt;sup>1</sup> The Group evaluates its risk exposure on a quarterly basis.

### 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 actions<sup>1</sup>.

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:



#### **LEGEND**

Probability:

(1) Rare; (2) Unlikely; (3) Moderate; (4) Possible; (5) Probable;

Impact:

- (1) Negligible; (2) Contained;
- (3) Significant; (4) Considerable; (5) Extreme.

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".

<sup>&</sup>lt;sup>1</sup> 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.).