RISK MANAGEMENT

Insight

TIM Group

June 2025

INDEX

1. Our Risk Management Model

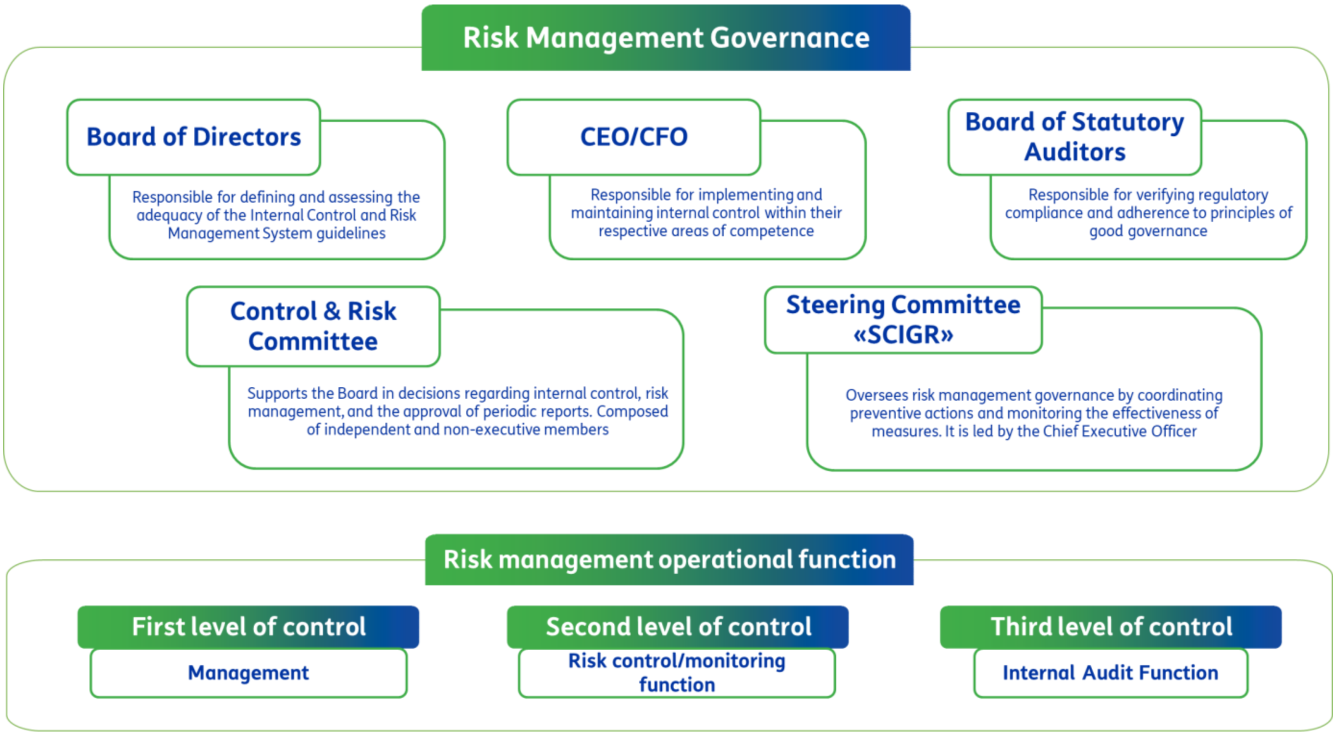
The model is based on a solid governance system entrusted to the Board of Directors, the Control and Risk Committee, and the Board of Statutory Auditors, which define the guidelines of the risk management system, assess its adequacy, oversee regulatory compliance, and ensure alignment with good governance principles.

Supporting governance is the "three lines of defense" model (i.e., three levels of management and control responsibilities):

- First line: represented by management, which identifies, assesses, and manages risks within operational activities;
- Second line: consisting of control and monitoring functions, which oversee the management process, define methodologies, and verify the implementation of mitigation measures;
- Third line: entrusted to the Internal Audit Department, which carries out an independent review of the effectiveness of the entire system, reporting directly to the governing bodies.

The Chief Executive Officer, supported by the Chief Financial Officer and the SCIGR Steering Committee (Internal Control and Risk Management System), coordinates the operational implementation of the Group's risk management model.

This integrated governance framework, summarized below, ensures constant and cross-functional oversight of business risks, strengthening the company's resilience and operational continuity.



Risk Management Governance

Board of Directors

Responsible for defining and assessing the adequacy of the Internal Control and Risk Management System guidelines

CEO/CFO

Responsible for implementing and maintaining internal control within their respective areas of competence

Board of Statutory Auditors

Responsible for verifying regulatory compliance and adherence to principles of good governance

Control & Risk Committee

Supports the Board in decisions regarding internal control, risk management, and the approval of periodic reports. Composed of independent and non-executive members

Steering Committee «SCIGR»

Oversees risk management governance by coordinating preventive actions and monitoring the effectiveness of measures. It is led by the Chief Executive Officer

Risk management operational function

First level of control

Management

Second level of control

Risk control/monitoring function

Third level of control

Internal Audit Function

Moreover, to promote a culture of risk awareness within the Company, we adopt a series of specific initiatives, including:

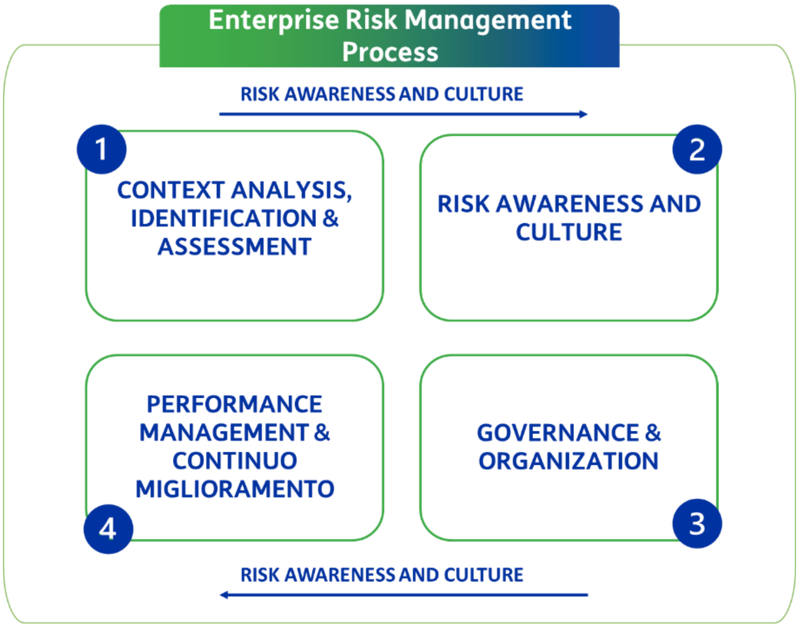
- regular activities to align and inform the Board of Directors on risk management and on the initiatives launched for their mitigation and monitoring;
- specialized risk management training courses, held annually, designed to strengthen an integrated risk perspective throughout the production chain and to provide continuous updates on the evolution of the subject and its applications within the company;
- periodic meetings with expert speakers in the field aimed at expanding knowledge on risk management;
- integration of risk criteria into the processes for developing products and services;
- alignment of remuneration policies with risk management objectives, through metrics linked to the Group's significant risks – including sustainability risks, such as customer satisfaction, engagement of young employees, and the gender pay gap – applied in the variable incentive system (MBO and LTI).

2. Risk Management Process

Within the TIM Group, the Enterprise Risk Management (ERM) process is structured as a continuous and integrated cycle, designed to ensure effective and proactive management of corporate risks. The process is divided into four main phases, supported by the cross-cutting promotion of a solid risk culture.

- Context analysis, identification, and assessment: We analyze the business context in relation to strategic objectives, identifying the main potential risks through tools such as the Risk Register, Heat Maps, and quantitative models useful for assessing their impact and likelihood. To understand and manage these risks effectively, we apply an integrated approach that allows us to break down the Strategic Plan into its key elements, highlighting volatility and critical areas. This direct link between strategy and risk enables us to ensure rigorous and dynamic control, supported by periodic updates and a continuous feedback flow from the Business Units and the Planning and Control function.
- Risk Appetite and management strategies: We evaluate the overall risk profile mapped together with the relevant Risk Owners, defining tolerance thresholds (Risk Appetite and Tolerance), treatment strategies (e.g., mitigation or transfer), responsibilities, and action plans. This phase is crucial to transform risk awareness into an operational strategy. To support the definition of Risk Appetite and management strategies, we use advanced quantitative models to analyze risk scenarios and event correlations, aiming to estimate the potential impact on the income statement and cash flow. These tools provide an objective basis for evaluating the corporate risk profile, contributing to more informed decisions and a more precise definition of intervention priorities.
- Governance and organization: The process is supported by a robust governance system led by the Board of Directors, which involves top management (three lines of defense) in decision-making.
- Performance management and continuous improvement: Finally, we work to integrate the risk culture into daily organizational life by developing new skills and promoting

conscious behaviors. The performance management system is oriented towards continuous improvement, aligned with the evolving context and emerging risks. At the same time, we adopt an adequate level of understanding of risks related to business and corporate processes to optimize results and strengthen the Group's responsiveness. A structured and conscious risk management approach also helps improve negotiating power in the market and safeguard operational continuity by keeping the impact of any adverse events within defined acceptable limits. Confirming the robustness of the system, the Group subjects the risk management process to quarterly internal audits, as well as external assessments entrusted to independent third parties (e.g., EY).

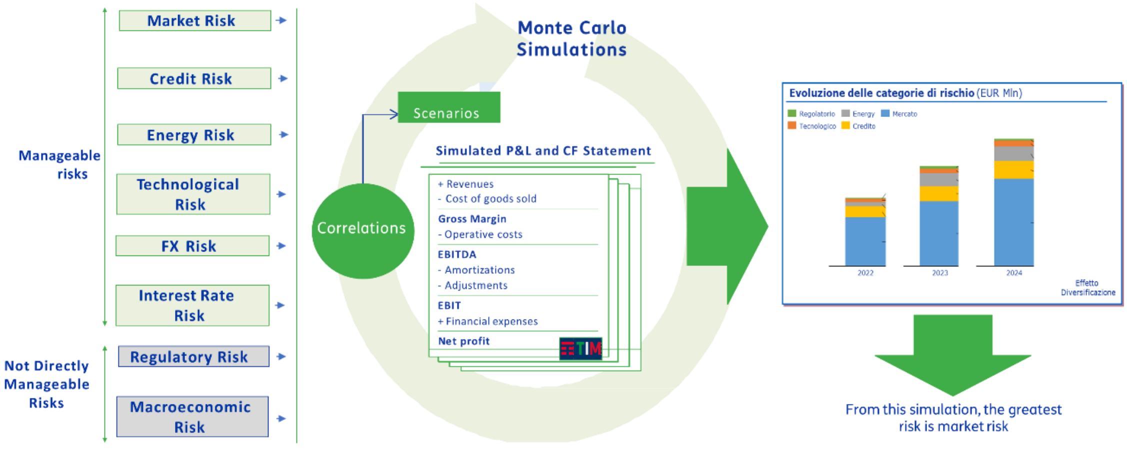

Enterprise Risk Management Process
RISK AWARENESS AND CULTURE
1
CONTEXT ANALYSIS, IDENTIFICATION & ASSESSMENT
2
RISK AWARENESS AND CULTURE
PERFORMANCE MANAGEMENT & CONTINUO MIGLIORAMENTO
4
GOVERNANCE & ORGANIZATION
3
RISK AWARENESS AND CULTURE

3. Quantitative Approach to Risk Assessment

In the risk assessment phase, in addition to qualitative analysis, we also adopt quantitative tools to objectively estimate the potential impact of different risk events. Among these, the Monte Carlo method plays a central role: it is a simulation model that, through the processing of thousands of scenarios built on statistical and probabilistic bases, makes it possible to quantify potential variations in the company's economic and financial results.

As illustrated in the diagram below, the process begins with the identification of the main risk categories, divided between those that can be managed (such as market, credit, technological, energy, currency, and interest rate risks) and those not directly controllable (such as regulatory and macroeconomic risks). From these categories, simulations are generated that incorporate correlations among the different risks, thereby producing a set of plausible scenarios. Each scenario allows us to estimate the effect on the income statement and cash flow: revenues, margins, EBITDA, EBIT, and net income.

The output of the simulation, shown in the chart on the right, displays the aggregated evolution of the contribution of each risk category to the company's economic performance over the years. The analysis highlights that, in the period under review, market risk represents the category with the greatest potential impact, followed by other categories with a smaller weight, thanks also to the diversification effect.

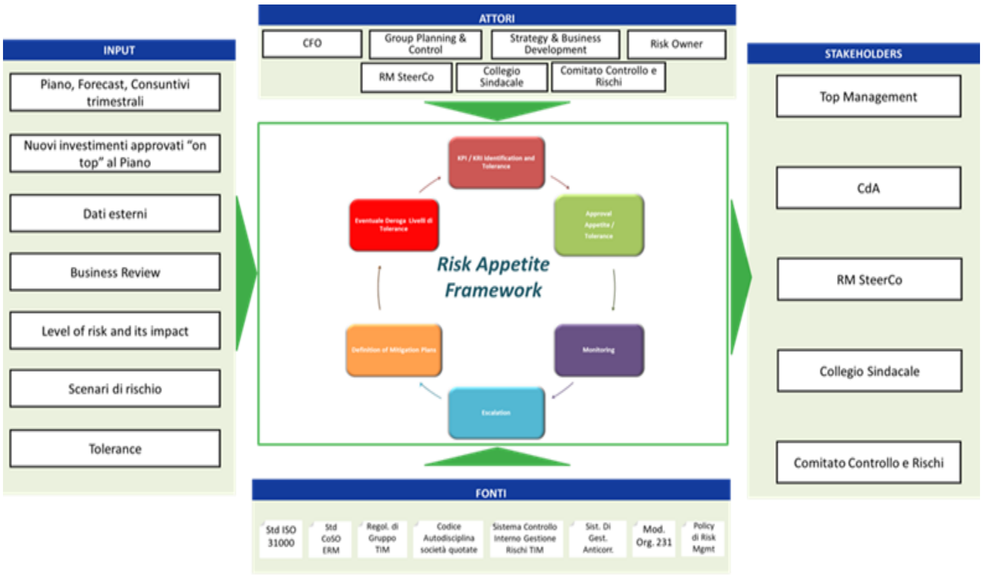


4. Integrated Risk Management: The Role of the Risk Appetite Framework

In our approach to Enterprise Risk Management, we use the Risk Appetite Framework (RAF) to define and represent the company's risk appetite in a structured way, aligned with the medium- to long-term strategic objectives outlined in the Industrial Plan. Specifically, this tool enables us to identify, assess, and monitor key risks through a methodology based on Key Risk Indicators (KRIs) and models that estimate both the probability of achieving expected performance and the impact of any deviations from predetermined targets.

The framework is structured as a continuous, cyclical process that begins with the definition of risk tolerance levels, continues with the approval of the Risk Appetite—namely, the level of risk the company is willing to accept—followed by results monitoring and possible escalation or exception in cases of threshold breaches, and concludes with the definition and implementation of mitigation plans.

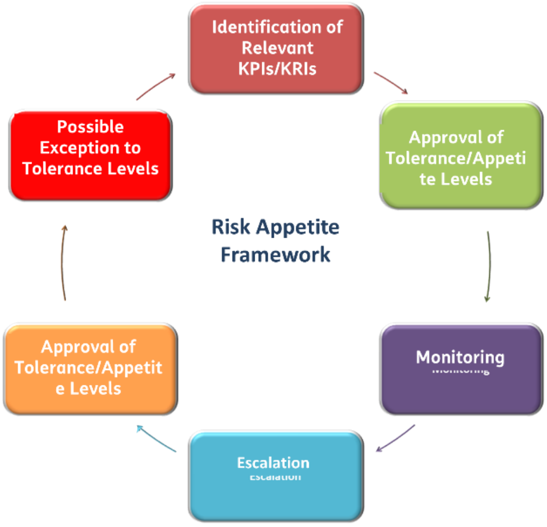
As illustrated in the following diagram, the RAF draws input from multiple sources: analysis of the Industrial Plan, forecast and actual data, approvals of extraordinary investments, market data, risk scenarios, and impact assessments.


ATTORI
CFO
Group Planning & Control
Strategy & Business Development
Risk Owner
RM SteerCo
Collegio Sindacale
Comitato Controllo e Rischi
INPUT
Piano, Forecast, Consuntivi trimestrali
Nuovi investimenti approvati "on top" al Piano
Dati esterni
Business Review
Level of risk and its impact
Scenari di rischio
Tolerance
KPI / KRI Identification and Tolerance
Approval Appetite / Tolerance
Monitoring
Escalation
Definition of Mitigation Plans
Eventuale Deroga Livelli di Tolerance
Risk Appetite Framework
STAKEHOLDERS
Top Management
CdA
RM SteerCo
Collegio Sindacale
Comitato Controllo e Rischi
FONTI
Std ISO 31000
Std CoSO ERM
Regol. di Gruppo TIM
Codice Autodisciplina società quotate
Sistema Controllo Interno Gestione Rischi TIM
Sist. Di Gest. Anticorr.
Mod. Org. 231
Policy di Risk Mgmt

The RAF actively involves several corporate functions (CFO, Group Planning & Control, Strategy & Business Development, Risk Owners) as well as oversight bodies (Control and Risk Committee, Board of Statutory Auditors), ensuring a cross-functional and shared oversight of risks. The outputs of the process are shared with key stakeholders, including Top Management, the Board of Directors, and the ERM Steering Committee.

The RAF is based on a comprehensive set of regulatory and normative references, including ISO 31000 and COSO ERM standards, the Organizational Model 231, the company's risk management policies, and the Corporate Governance Code for listed companies. The outputs of the process feed into our strategic and operational decisions, guiding the development of targeted mitigation actions and contributing to an effective balance between risk and return.

In detail, our RAF cycle is structured into six operational phases:

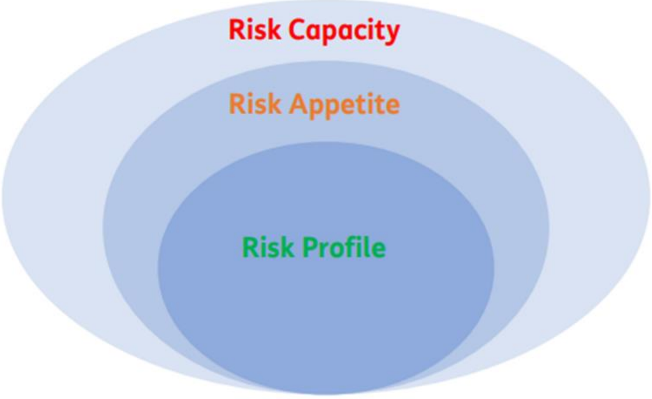

Identification of Relevant KPIs/KRIs
Approval of Tolerance/Appetite Levels
Monitoring
Escalation
Approval of Tolerance/Appetite Levels
Possible Exception to Tolerance Levels
Risk Appetite Framework

1. **Identification of Relevant KPIs/KRIs and Proposed Appetite/Tolerance Levels:** The ERM function analyzes the Strategic Plan data and, based on the estimated risk levels (@Risk), proposes the relevant objectives along with their corresponding appetite and tolerance thresholds.

2. **Approval:** The proposed appetite/tolerance levels are reviewed with the CFO and submitted to the Control and Risk Committee, before being approved by the Board of Directors.
3. **Monitoring:** On a quarterly basis, or upon request, we monitor the approved levels through the analysis of updated forecast, actual, and business data. Business Plans also incorporate new strategic projects, which are assessed using quantitative models and Monte Carlo simulations to evaluate their impact on the likelihood of achieving objectives.
4. **Escalation**: In the event of a breach of the defined levels, the ERM function initiates an escalation process, involving the Risk Owner to assess the risk exposure and define corrective actions.
5. **Mitigation Plans:** We define and implement targeted plans aimed at bringing risk levels back within acceptable limits.
6. **Exception:** In selected and formally authorized cases, an exception to the tolerance levels may be granted.

Our RAF is based on a set of well-defined concepts that guide risk management:

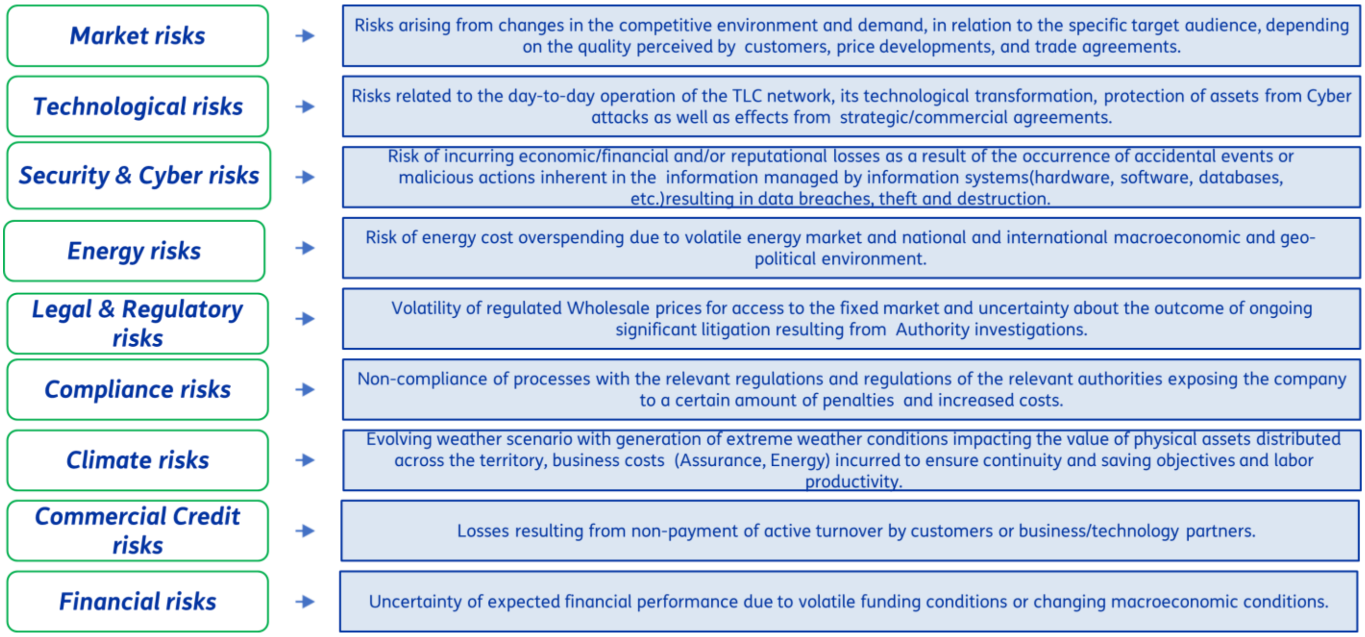
- Risk Capacity: This is the maximum level of risk we are technically able to bear without compromising business continuity.
- Risk Appetite: This represents the overall level of risk we are willing to accept in order to pursue our strategic objectives.
- Risk Tolerance: This indicates the maximum deviation from objectives that we consider tolerable without jeopardizing their achievement, nor exposing ourselves to losses, operational issues, or reputational damage.
- Risk Profile: This is the actual level of risk currently assumed by the Company at a given point in time.



The graphic representation highlights how the risk profile must remain within the boundaries defined by the risk appetite, which, in turn, should never approach the threshold of the risk capacity. The tolerance acts as a safety buffer, beyond which control or mitigation mechanisms are triggered.

5. Mapping, Classification and Prioritization of Risks

In our integrated risk management system, we adopt a methodology that starts with mapping and classifying the main risk areas, followed by the assessment of their likelihood and potential impact, and then prioritization within a dynamic matrix. This approach offers a structured view and up-to-date view of our overall risk exposure, with the goal of effectively guiding mitigation and control activities.



Market risks	Risks arising from changes in the competitive environment and demand, in relation to the specific target audience, depending on the quality perceived by customers, price developments, and trade agreements.
Technological risks	Risks related to the day-to-day operation of the TLC network, its technological transformation, protection of assets from Cyber attacks as well as effects from strategic/commercial agreements.
Security & Cyber risks	Risk of incurring economic/financial and/or reputational losses as a result of the occurrence of accidental events or malicious actions inherent in the information managed by information systems(hardware, software, databases, etc.)resulting in data breaches, theft and destruction.
Energy risks	Risk of energy cost overspending due to volatile energy market and national and international macroeconomic and geo-political environment.
Legal & Regulatory risks	Volatility of regulated Wholesale prices for access to the fixed market and uncertainty about the outcome of ongoing significant litigation resulting from Authority investigations.
Compliance risks	Non-compliance of processes with the relevant regulations and regulations of the relevant authorities exposing the company to a certain amount of penalties and increased costs.
Climate risks	Evolving weather scenario with generation of extreme weather conditions impacting the value of physical assets distributed across the territory, business costs (Assurance, Energy) incurred to ensure continuity and saving objectives and labor productivity.
Commercial Credit risks	Losses resulting from non-payment of active turnover by customers or business/technology partners.
Financial risks	Uncertainty of expected financial performance due to volatile funding conditions or changing macroeconomic conditions.

As shown in the figure above, the risks we consider are organised into eleven main categories, including:

- **Market risks,** related to demand trends and competitive changes;
- **Technological risks**, related to the operation and evolution of the TLC network;
- **IT and security risks**, related to cyber threats, data theft or destruction;
- **Energy and climate risks**, arising from market volatility and environmental conditions;
- **Legal and regulatory risks**, related to regulatory uncertainties and litigation;
- **Financial, credit and exchange rate risks**, attributable to macroeconomic conditions, solvency and currency fluctuations.

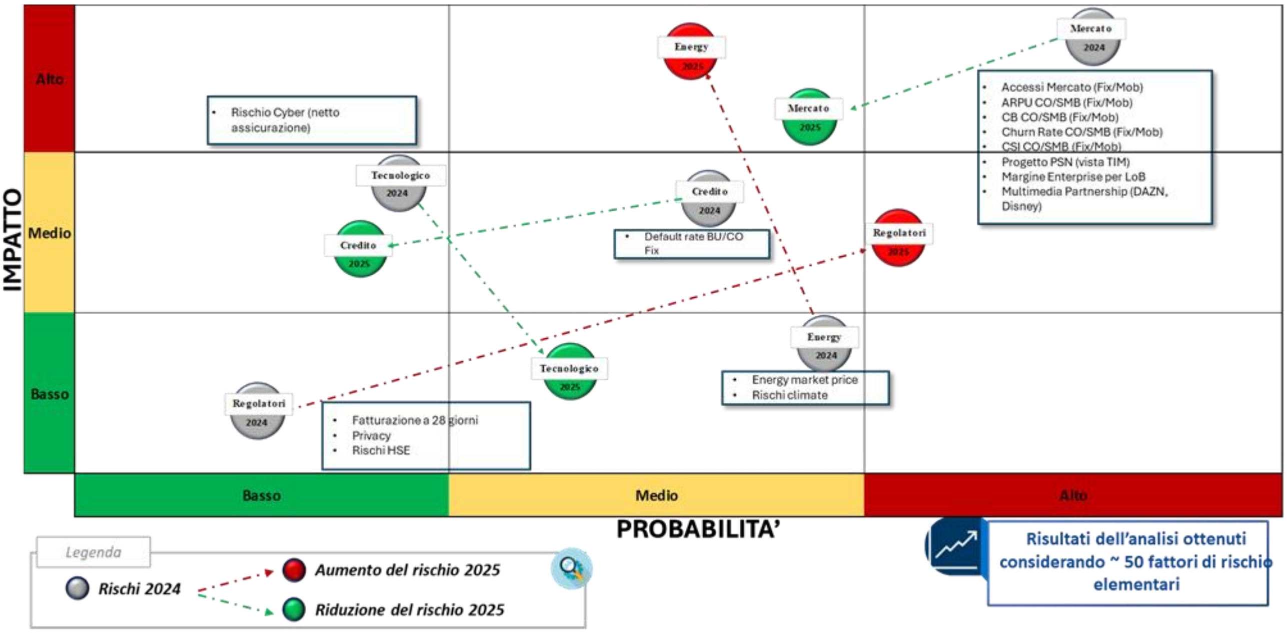
For each category, we define the tolerance level and estimate the probability and extent of the potential impact using assessment models supported by approximately 50 basic risk factors.

As shown in the figure above, the risks we consider are organized into eleven main categories, including:

- **Market risks**, related to demand trends and competitive changes;

- **Technological risks**, concerning the operation and evolution of the telecommunications network;
- **Cybersecurity and information security risks**, linked to cyber threats, data theft, or destruction;
- **Energy and climate risks**, arising from market volatility and environmental conditions;
- **Legal and regulatory risks**, connected to regulatory uncertainties and litigation;
- **Financial, credit, and exchange rate risks**, attributable to macroeconomic conditions, solvency, and currency fluctuations.

For each category, we define the tolerance level and estimate the probability and magnitude of potential impact through evaluation models supported by approximately 50 elementary risk factors.



The results of our analysis are then represented within a risk matrix, as illustrated in the second image. Each risk is positioned according to its probability level (horizontal axis) and impact (vertical axis) and marked with a label indicating its category and time horizon (e.g., 2024 or 2025), to support effective long-term planning. Risks are distributed across three severity levels:

- Low (green): tolerable without urgent action;
- Medium (yellow): subject to monitoring and preventive measures;
- High (red): requiring priority interventions.

A few examples highlight our current priorities:

Cyber risk, although partially mitigated through insurance, is positioned in the red area due to its high potential impact on operational continuity.

Market risks are spread across different levels, depending on access dynamics, churn rate, and average revenues.

Energy, regulatory, and trade credit risks vary in importance based on the evolution of the external and regulatory context.

We update the matrix on a quarterly basis, drawing on forecast data, actual results, and scenario analyses, in order to ensure continuous and responsive oversight. This approach enables us to anticipate critical issues, strengthen mitigation measures, and optimize the allocation of resources within control mechanisms, in line with our risk appetite and our long-term objectives of sustainability, resilience, and value creation.

6. Analysis and Management of the Most Significant Risks

Building on the risk matrix presented in the previous section, which visually represents the positioning of risks based on a combined assessment of likelihood of occurrence and potential impact, we provide below a more detailed analysis of two significant risks for our Group: market risk and energy risk. For each, we describe the methodologies used for impact assessment and the main mitigation actions adopted.

Market Risk

The evolution of the competitive landscape and demand—driven by factors such as service pricing, customer-perceived quality, and the dynamics of commercial agreements—represents a critical element in our market risk analysis. To assess its impact, we use a combination of deterministic and probabilistic quantitative models, including:

- Constrained optimization method;
- Monte Carlo simulations for probabilistic analysis;
- Game Theory model (Nash Equilibrium);
- CashFlow@Risk model, focused on impacts against the Industrial Plan targets;
- NPV@Risk model (via VOSE ModelRisk software) for evaluating risks associated with industrial investment projects.

To mitigate the impact of identified risks, we have implemented several initiatives, including:

- Convergent offers with partners such as DAZN, Netflix, and Disney+, enhancing perceived value and strengthening customer loyalty;
- Continuous network quality improvements, supported by investments in infrastructure, including the 5G network;
- Targeted acquisition campaigns aimed at customers migrating from other operators;
- Ongoing monitoring of price/quality positioning, ensuring competitiveness in line with market dynamics.

Energy Risk

The impact of energy risk, stemming from the volatility of energy prices and the evolution of the macroeconomic and geopolitical context, is also monitored with the utmost attention. To assess this risk, we employ:

- Probabilistic model, which simulates energy price trends by integrating elements of trend and volatility;

- Quantification is performed by measuring the distance between the 5th percentile of the simulated price and the value forecast in the Plan, in order to obtain a robust and prudent estimate.

Mitigation measures adopted include:

- Establishing a policy for managing energy hedges, which provides for the use of forward contracts and derivative instruments to stabilize costs;
- Continuous monitoring of risk, with analyses periodically shared among the relevant functions—particularly Planning & Control and Finance—at least on a quarterly basis.

Through these activities, we maintain an active and integrated control of our risk profile, ensuring alignment with our objectives of economic sustainability and operational stability.

7. Identification and management of emerging risks

In continuity with the assessment of priority risks, we broaden our perspective to include phenomena that, although not yet fully manifested, may have significant impacts in the medium to long term (3–5 years). These emerging risks represent, in line with the World Economic Forum model, new types of "disruptive" risks that are difficult to quantify and long-lasting.

In the following subsections, we examine three emerging risks of particular relevance for the TIM Group, also addressing the impacts and the mitigation measures adopted.

Risks and Challenges Arising from the Adoption of Artificial Intelligence

In our corporate context, the adoption of Artificial Intelligence (AI) solutions and systems is steadily increasing, in line with the technological evolution transforming the telecommunications sector. AI represents a strategic lever for us, capable of generating operational efficiencies and fostering innovation, while at the same time introducing new and complex risks that require careful, responsible, and forward-looking management.

Challenges: the integration of AI into our business processes presents several operational and systemic challenges, including:

- Availability of adequate budget;
- Compliance with national and European regulatory frameworks;
- Management of data and infrastructure security;
- Shortage of specialized expertise to design, implement, and govern AI solutions;
- Data quality and integrity;
- Big data analysis and real-time decision-making capabilities;
- Interoperability and adequacy of technological infrastructure;
- Difficulties in integrating with existing systems;
- Limitations in technology sourcing;
- The need to ensure transparency, reliability, and trust among stakeholders.

Threats: In addition to these challenges, we acknowledge that the use of AI technologies also entails specific threats, including:

- Breaches of privacy and personal data security;
- Non-compliance with intellectual property and copyright regulations;
- Algorithmic discrimination and bias in AI system outputs;
- Exposure to cybersecurity risks linked to the functioning of intelligent systems.

Potential Impacts: The potential consequences associated with these risks may be economic, legal, and reputational. In particular, regulatory impact is one of the most significant aspects. Non-compliance with the new European AI Regulation (AI Act) may result in substantial financial penalties — up to 7% of annual global turnover for the use of prohibited AI systems, and up to 3% for failure to meet the requirements applicable to high-risk classified systems.

In addition to the risk of penalties, there is also the potential risk of not achieving the expected benefits from AI investments, due to lower-than-expected revenues or higher costs incurred for the development, maintenance, or correction of the implemented solutions.

Mitigation actions: To address these challenges in a systemic way, we have chosen to adopt a centralized AI governance model, aligned with the objectives of our Strategic Plan. We have established a multifunctional team, composed of experts from various corporate functions (e.g. Strategy, Finance, Compliance, Legal, Security, etc.), to ensure integrated and consistent management of AI, considering its technical and organizational complexity.
Our main mitigation actions include:

- Defining policies and procedures to regulate the responsible use of AI, while promoting an ethical culture and greater awareness among Clients, Suppliers, and Employees.
- Adopting a centralized governance structure with clearly defined roles and responsibilities, ensuring effective oversight throughout the entire AI system lifecycle.
- Creating and maintaining an up-to-date inventory of all AI models and systems used within the Group, including the data utilized and the logic implemented.
- Implementing a risk classification tool for each AI system, in compliance with the categories and requirements set out in the AI Act.
- Integrating a structured risk management process across the entire lifecycle of AI solutions — from design and development to testing and deployment. This model foresees:
    - Preventive measures, based on the principle of "ethics by design";
    - Ex-post measures, including continuous monitoring, human oversight, and periodic reviews of AI system performance, to promptly detect biases and correct anomalies.

Ultimate goal is to ensure that every AI system is designed and managed in full respect of individuals' fundamental rights, guaranteeing maximum safety for both people and the corporate assets and processes involved.

Transition Risk: Introduction of a Carbon Tax

As part of our Enterprise Risk Management process, we have included the emerging environmental risk associated with the introduction of a Carbon Tax on CO_2 emissions. This regulatory and financial risk is closely linked to the global transition toward a low-emission economy and could generate significant additional costs for our operations, particularly in relation to decarbonization initiatives.

Threats: We conducted an in-depth analysis of activities and assets potentially incompatible with a Net Zero strategy, assessing their alignment with Delegated Regulation (EU) 2021/2139 and the criteria of the EU Taxonomy. The critical issues identified include:

- Management of data centers and network infrastructures;
- Direct and indirect energy consumption;
- Dependence on fossil fuels within the supply chain.

Potential Impacts: The potential impact has been quantified through scenario analyses — both qualitative and quantitative — inspired by the NGFS (Network for Greening the Financial System) framework, with the aim of aligning our climate strategy to the 1.5 °C global warming limit. In particular:

- We estimated a reference average carbon tax price of €83.5 per tCO_2 (for 2024);
- A linear projection of emissions reduction was carried out through 2040, with decadal milestones;
- We assessed the economic impacts in the event of failing to meet targets, with deviations of 10%, 20%, and 30%;
- We also considered the effects of extreme climate events that could compromise the operational continuity of our services.

Mitigation Actions: To limit our exposure to this risk and anticipate potential negative impacts, we have implemented a series of targeted initiatives, including:

- Certification of our Environmental Management System in accordance with ISO 14001 and commitment to science-based targets defined under the SBTi methodology;

- Bringing forward to 2025 the goal of sourcing 100% renewable electricity for all Italian operations (already achieved in Brazil);
- A national plan of interventions for upgrading infrastructures and cooling systems, aimed at reducing emissions and improving energy efficiency;
- Modernization of technological assets in industrial buildings, with priority given to strategic sites, to ensure long-term resilience and sustainability;
- Adoption of an Energy Management System (BEMS) with IoT devices for monitoring and predictive maintenance of technological systems;
- Active engagement of suppliers through the introduction of stricter ESG criteria in production processes, in order to reduce indirect emissions across the supply chain.

Through these actions, we strengthen our commitment to a fair and sustainable transition, reducing our exposure to future environmental costs and increasing the resilience of our operations.

Cyber Threat Risks and Impacts Linked to the Geopolitical Context

In an increasingly interconnected world, cyber risk — amplified by geopolitical tensions and evolving European regulations — represents one of the most critical challenges to the security of our business. The growing reliance on digital technologies and IT infrastructures increases our exposure to complex and sophisticated cyber threats, with potential impacts on assets, data, and reputation.

Threats: The World Economic Forum has identified cross-border cyberattacks among the most critical areas of emerging risk. In this context, the adoption of legislative measures by the EU — such as the NIS2 Directive and the proposed Cybersecurity Act — aims to strengthen the resilience of critical sectors, including telecommunications.

Potential impacts:

- Disruption of asset availability supporting ICT services;
- Regulatory sanctions for data breaches and non-compliance with legislation (e.g., NIS2);

- Loss of trust from clients, especially institutional and strategic ones;
- Reputational and financial damage in the event of geopolitically motivated attacks.

In 2024, we recorded a single medium-impact cyber incident (a DDoS attack), which was promptly contained without any data loss or disruption to the public network. Two additional minor episodes had no significant economic or operational consequences.

Mitigation actions: to ensure effective and continuous oversight of cybersecurity, we have adopted a proactive and structured approach, which includes:

- Regular risk assessments, including penetration testing, vulnerability assessments, and the use of the FAIR (Factor Analysis of Information Risk) methodology for economic quantification of cyber risks;
- A 24/7 Security Operations Center (SOC) capable of detecting, preventing, and responding promptly to any threat;
- ISO 22301 certification for business continuity management, ensuring the resilience of the services provided;
- ISO 27001 certification for information security, along with advanced cryptographic systems to safeguard sensitive data;
- Corporate Data Recovery policies, ensuring the storage and protection of backups not exposed to public networks;
- Continuous monitoring of regulatory compliance, carried out by the Compliance function in close coordination with all functions involved in digital processes.

Through these measures, we actively address emerging cyber threats, safeguard stakeholder trust, and ensure the continuity and reliability of our services.