



RISK MANAGEMENT

Insight

TIM Group

September 2026



INDEX

1. Tim Group's Risk Management model	3
2. The Risk Management model	6
3. A quantitative approach to risk management	7
4. Integrated Risk Management: the role of Risk Appetite Framework	9
5. Risk Mapping, Classification and Prioritization	13
6. Analysis and Management of the most relevant risks	15
7. Recognition and Management of emerging risks	19



1. Tim group's Risk Management model

At TIM Group, we adopt a structured Enterprise Risk Management (ERM) model, based on the international ISO 31000:2018 standards and the COSO Framework, with the goal of systematically identifying, assessing, managing, and monitoring business risks.

We promote a risk culture that extends to all levels of the organization, and our approach is based on several fundamental principles:

- **alignment with strategy and objectives:** we take into account the internal and external context in which we operate, integrating the ERM process into the corporate strategy to support the achievement of key objectives, including economic and financial ones;
- **integration and collaboration:** we treat the ERM process as an integral part of our daily activities and foster cooperation among different functions, bringing together technical and business expertise;
- **agility and adaptability:** we recognize that risks change over time. That is why we constantly monitor the evolution of risk factors and take mitigation measures when necessary.
- **analytical approach:** where possible, the ERM process uses quantitative assessment methods, based on impact and probability of occurrence.
- **comprehensive overview:** We don't just analyze risks individually, but also as a set of interrelated factors, to gain a more comprehensive view.
- **improvement over time:** we regularly update and review the ERM process to ensure it remains effective and aligned with best practices.

The ERM process is managed on an ongoing basis, is cyclical in nature, and is pervasive throughout the organization, as it involves all corporate functions and key stakeholders.

The Risk Management System adopted by TIM is based on a robust governance framework, in which the **Board of Directors, the Control and Risk Committee, and the Board of Statutory Auditors** ensure its adequacy, monitor regulatory compliance, and verify alignment with the principles of good governance.



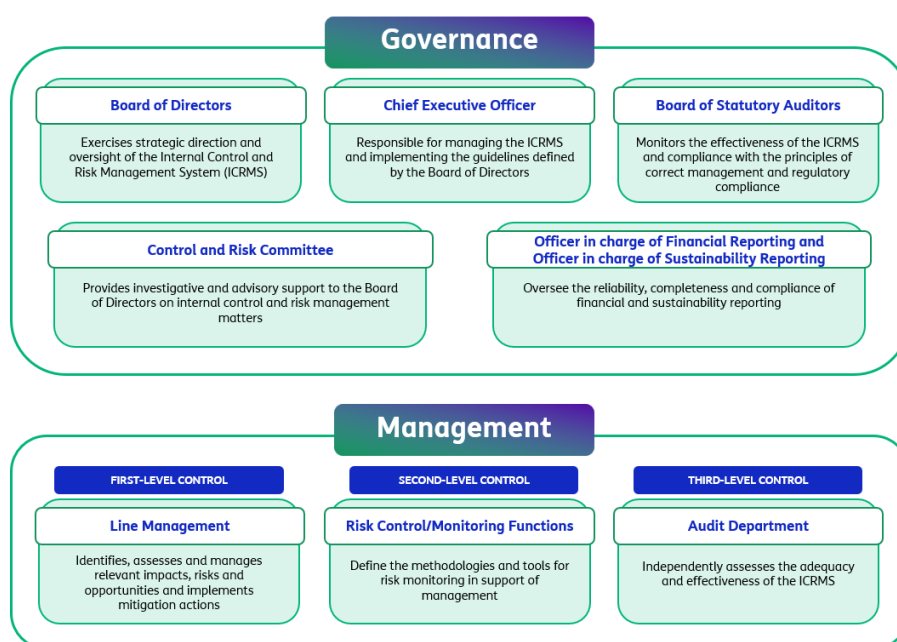
The “**three lines of defense**” model (i.e., three lines of management and control responsibility) supports governance:

- **the first line**, represented by **management**, identifies, assesses, and manages risks within operational activities;
- **the second line**, consisting of **control and monitoring functions**, supervises the management process, defines methodologies, and verifies the implementation of mitigation measures;
- **the third line** is entrusted to the **Internal Audit Department**, which independently verifies the effectiveness of the entire system and reports directly to the governing bodies.

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

This integrated governance model, summarized below, ensures constant, cross-functional oversight of corporate risks, thereby supporting the company’s financial strength and operational continuity.

Risks of greater strategic importance or with cross-functional impacts are overseen by the ERM Steering Committee, which supports the CFO in managing the Group’s risk profile.



Moreover, to foster a culture of risk awareness within the company, we implement a series of specific initiatives, including:

- regular efforts to coordinate with and keep the Board of Directors informed regarding risk management and the initiatives undertaken to mitigate and monitor risks, complemented by regular risk management education and training provided to all non-executive directors to ensure that they remain updated on the Group's key risks, risk management principles and relevant developments;
- specialized training courses on risk management education and principles, held annually across the organization, designed to strengthen an integrated view of risk throughout the Group and its value chain and provide ongoing updates on developments in the field and their application within the company;
- regular meetings with experts in the field, with the aim of expanding knowledge of risk management;
- integration of risk criteria into product and service development processes;
- alignment of compensation policies with risk management objectives, through metrics linked to risks relevant to the Group, including sustainability risks, such as customer



satisfaction, the engagement of young employees, and the gender pay gap, applied in the variable incentive system (MBO and LTI).

2. The Risk Management process

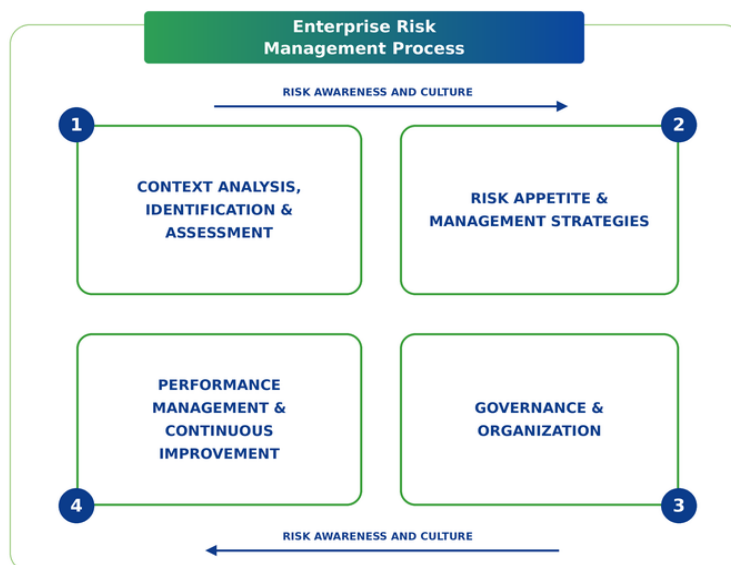
Within the TIM Group, the Enterprise Risk Management (ERM) process is structured as a continuous and integrated cycle, designed to ensure effective and proactive management of corporate risks. The process consists of four main phases, supported by the cross-functional promotion of a robust risk culture.

1. **Context Analysis, Identification, and Assessment:** we analyze the business context in relation to strategic objectives, identifying the main potential risks using tools such as the Risk Register, Heat Maps, and quantitative models to assess their impact and probability. 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 their volatility and critical areas. This direct link between strategy and risk enables us to ensure rigorous and dynamic control, thanks to periodic updates and a continuous flow of feedback from the Business Units and the Planning and Control function.
2. **Risk Appetite and Management Strategies:** we assess the overall profile of the identified risks together with the relevant Risk Owners, defining tolerance thresholds (Risk Appetite and Tolerance), treatment strategies (such as mitigation or transfer), responsibilities, and action plans. This phase is essential for transforming 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 correlations between events, with the goal of estimating the potential impact on the income statement and cash flow. These tools provide an objective basis for assessing the company's risk profile, helping to support more informed decisions and define any priorities for action.
3. **Governance and Organization:** The process is supported by a robust governance framework established by the Board of Directors, which provides for the involvement of top management (three lines of defense) in the decision-making process.



4. **Performance Management and Continuous Improvement:** Finally, we work to integrate a risk culture into our day-to-day operations by developing new skills and promoting mindful behavior. Our performance management system is geared toward continuous improvement, in line with changes in the business environment and emerging risks.

At the same time, we ensure an adequate level of understanding of the risks associated with our business and corporate processes, in order to optimize results and strengthen the Group's ability to respond. A structured and informed approach to risk management also helps improve our negotiating position in the market and safeguard business continuity, keeping the impact of any adverse events within defined acceptable limits. As further evidence of the system's robustness, the results of the ERM process analyses are also shared periodically with the Internal Audit Department.



3. A Quantitative Approach to Risk Assessment

During the risk assessment phase, in addition to qualitative analysis, we also use quantitative tools to objectively estimate the potential impact of various risk events. Among these, the Monte Carlo method is a key technique: it is a simulation model that, by processing thousands



of scenarios based on statistics and probability, allows us to quantify possible variations in the company's financial and economic results.

As illustrated in the diagram below, the process begins with the identification of the main risk categories, distinguished between those that are manageable (such as market, credit, technology, energy, currency, and interest rate risks) and those that are not directly controllable (such as regulatory and macroeconomic risks). Based on these, simulations are generated that incorporate the correlations between the various risks, thereby producing a series of plausible scenarios. Each scenario allows for an estimation of the impact on the income statement and cash flow: revenue, margins, EBITDA, EBIT, and net income.

The simulation results, shown in the graph below, illustrate the aggregate evolution of each risk category's contribution to economic performance over the years. The analysis shows that, during the period under review, market risk is the component with the greatest potential impact, followed by other categories with a lesser impact, thanks in part to the effect of diversification.



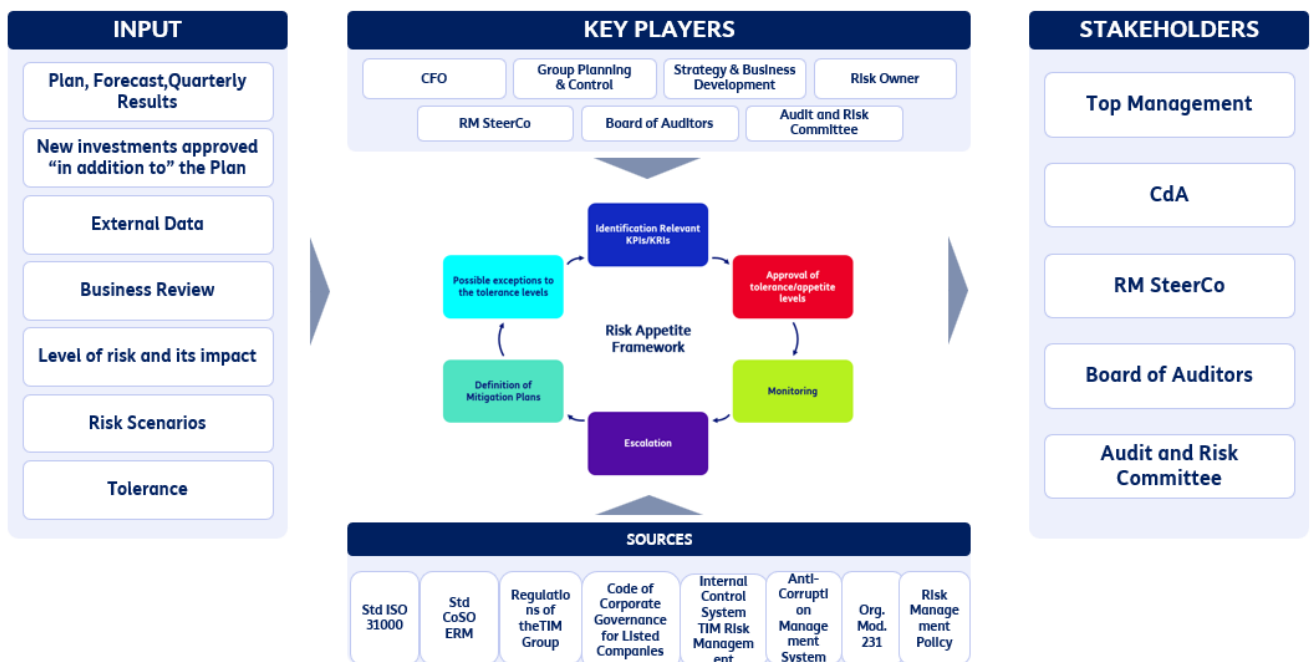


4. Integrated Risk Management: the Role of the Risk Appetite Framework

In our approach to Enterprise Risk Management, we use the **Risk Appetite Framework (RAF)** to define and structurally represent the company's risk appetite, in line with the medium- to long-term strategic objectives set out in the Business Plan. Specifically, this tool allows us to identify, assess, and monitor key risks through a methodology based on Key Risk Indicators (KRIs) and models that estimate the probability of achieving expected performance, as well as the impact of any deviations from the set targets.

The framework translates into a cyclical and continuous process that begins with defining risk tolerance levels, continues with the approval of the Risk Appetite, i.e., the level of risk the company is willing to accept, and the related operational thresholds for preventive alert (Early Warning), tolerance (Tolerance), and critical status (Stress); the monitoring of results and any escalation or exception in cases where thresholds are exceeded; and concludes with the definition and implementation of mitigation plans.

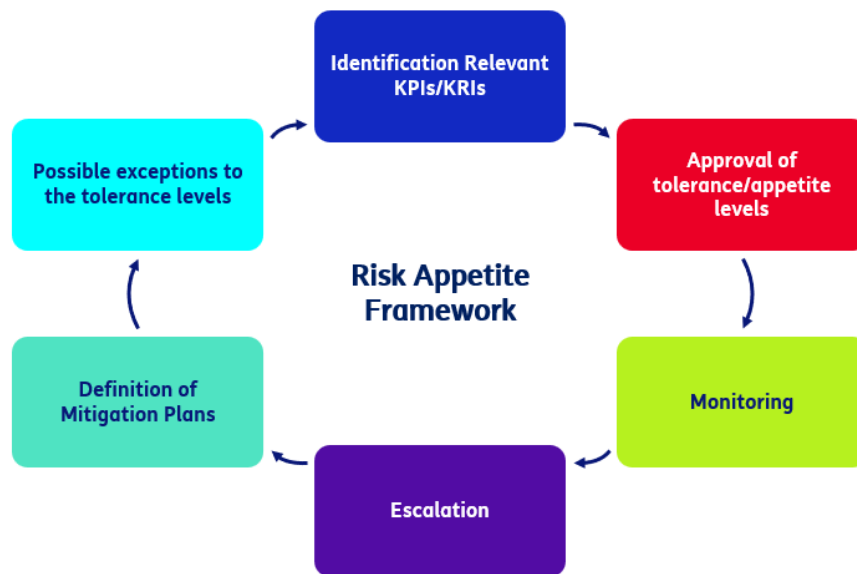
As shown in the image below, the Risk Appetite Framework draws on inputs from multiple sources: analysis of the business plan, forecast and actual data, approvals of extraordinary investments, market data, risk scenarios, and impact assessments.



The RAF actively involves various corporate functions (CFO, Group Planning & Control, Strategy & Business Development, Risk Owner) and control bodies (Control and Risk Committee, Board of Statutory Auditors), ensuring cross-functional and shared risk oversight. 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 the ISO 31000 and COSO ERM standards, the 231 Organizational Model, corporate risk management policies, and the Corporate Governance Code for listed companies. The outputs of the process inform our strategic and operational decisions, guiding the development of targeted mitigation actions and helping to ensure an effective balance between risk and return.

Going into more detail, the Risk Appetite Framework is structured into **six operational phases**:

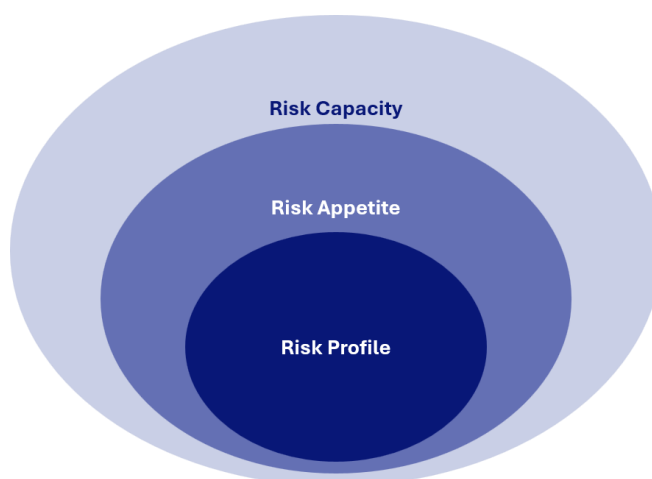


1. **Identification of relevant KPIs/KRIs and proposed appetite/tolerance levels:** the ERM function analyzes the data from the Strategic Plan and, based on the estimated risk levels (@Risk), proposes the objectives considered relevant along with the related appetite and tolerance levels.
2. **Approval:** the appetite/tolerance levels are shared 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. We also include new strategic projects in the Business Plans, which we simulate using quantitative models and Monte Carlo analysis to assess their impact on the probability of achieving the objectives.
4. **Escalation:** if the defined levels are exceeded, the ERM function activates an escalation process, involving the Risk Owner to assess the risk exposure and define corrective actions.
5. **Mitigation plans:** we define and implement plans aimed at bringing risk levels back within acceptable limits
6. **Exception:** in select and formally authorized cases, we may allow an exception to the tolerance levels, while still maintaining oversight through ongoing monitoring.



The RAF adopted by the company is based on a set of clearly distinct concepts that guide risk management:

- **Risk Capacity:** the maximum level of risk we are technically able to bear without compromising business continuity.
- **Risk Appetite:** represents the overall level of risk we are willing to accept in order to pursue our strategic objectives.
- **Risk Tolerance:** indicates the maximum deviation from objectives that we consider tolerable without compromising their achievement, or exposing ourselves to losses, operational issues, or reputational damage.
- **Risk Profile:** the amount of risk actually assumed by the Company at a given point in time.



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



5. Risk Mapping, Classification, and Prioritization

In our integrated ERM risk management system, we adopt a methodology that involves mapping and classifying the main risk areas, assessing their probability and potential impact, and subsequently prioritizing them in a dynamic matrix. This approach provides a structured and up-to-date view of overall risk exposure and effectively guides mitigation and control activities.

In line with the evolving regulatory, technological, and business landscape, the ERM framework continuously monitors emerging risks and drivers of change that may alter the company's risk profile.

Below are the main risk areas identified by the TIM Group:

Market Risks	Risks arising from changes in the competitive environment and in demand, as they relate to the specific target audience, depending on customers' perception of quality, price trends, and commercial agreements.
Technological Risks	Risks related to the day-to-day operation of the TLC network, its technological transformation, the protection of assets from cyberattacks, and the effects of strategic and commercial agreements.
Cybersecurity and Security Risks	Risk of incurring economic/financial and/or reputational losses as a result of accidental events or malicious acts involving information managed by IT systems (hardware, software, databases, etc.) that lead to data breaches, theft, and destruction.
Energy Risks	Risk of energy costs exceeding budget due to volatility in the energy market and in the national and international macroeconomic and geopolitical environment.
Legal and Regulatory Risks	Volatility in regulated wholesale prices for fixed-line market access and uncertainty regarding the outcome of significant ongoing disputes arising from the Authority's guidance.
Compliance Risks	Non-compliance of processes with relevant laws and regulations and the rules set by the competent authorities, which exposes the company to a certain amount of penalties and increased costs.
Climate Risks	A changing weather scenario is giving rise to extreme weather conditions that impact the value of physical assets distributed throughout the territory, the business costs (insurance, energy) incurred to ensure continuity and meet cost-saving targets, and labor productivity.
Commercial Credit Risks	Losses resulting from the failure of customers or business/technology partners to pay outstanding invoices.
Financial Risks	Uncertainty regarding expected financial performance due to volatile financing conditions or changes in macroeconomic conditions.
Exchange Rate Risks	Fluctuations in the exchange rates of various currencies relative to the consolidation currency (the euro), which may result in changes in consolidated equity; and fluctuations in currency exchange rates arising from the measurement and translation of trade receivables (payables).
Risks Associated with Artificial Intelligence	Risks arising from the adoption and use of artificial intelligence systems, with particular reference to transparency, reliability, security, algorithmic bias, data protection, regulatory compliance (AI Act), and adherence to ethical and fairness principles.
Supply Chain Risks	Risks arising from supply chain management, with particular reference to supplier resilience, compliance with ESG principles, human rights, environmental and social regulations, and supply continuity.

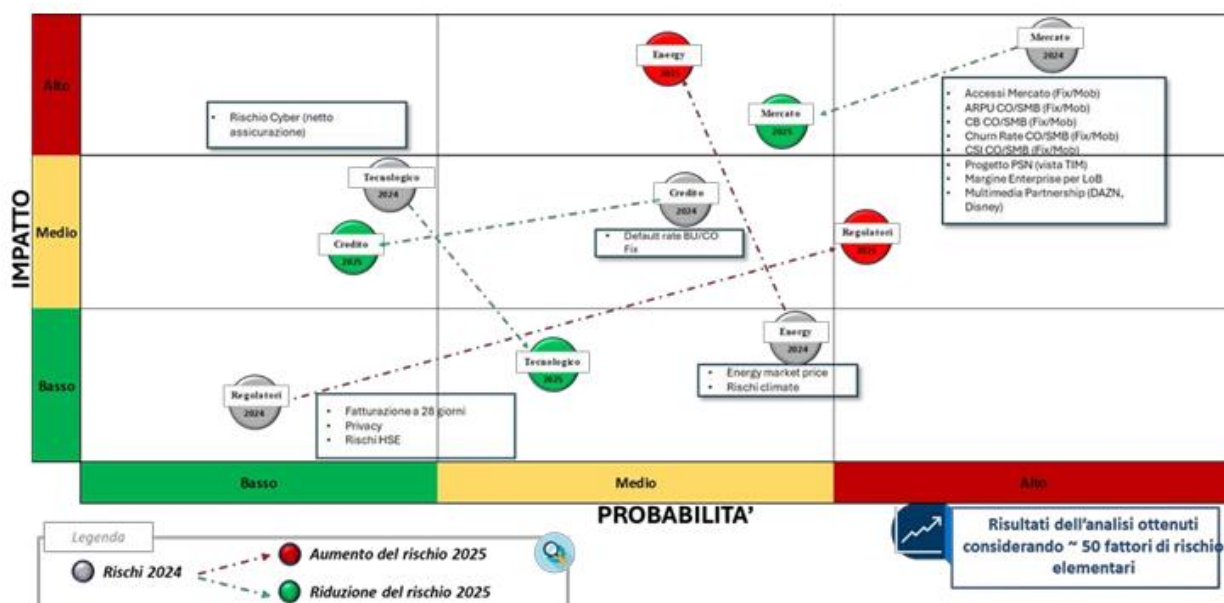
As shown previously, the risks we consider are organized into the following main categories:

- **Market risks**, related to demand trends and competitive changes;
- **Technological risks**, relating to the operation and evolution of the TLC network;



- **IT and security risks**, linked to cyber threats, data theft, or destruction;
- **Energy and climate risks**, arising from market volatility, environmental conditions, and climate change;
- **Legal and regulatory risks**, connected to regulatory uncertainty and litigation;
- **Financial, credit, and exchange rate risks**, attributable to macroeconomic conditions, solvency, and currency fluctuations;
- **Risks related to Artificial Intelligence**, concerning transparency, reliability, algorithmic bias, security, data protection, regulatory compliance, and adherence to ethical and fairness principles;
- **Supply chain risks**, connected to operational continuity, supplier reliability, cost volatility, regulatory compliance, and environmental and social impacts, including the protection of human rights and adherence to ESG standards.

For each category, we define the tolerance level and estimate the probability and magnitude of the 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 shown in the second image. Each risk is positioned according to its probability level (horizontal axis) and impact level (vertical axis), and marked with a label indicating its category and time horizon (e.g., 2025 or 2026), in order 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 action;
- **High (red):** requiring priority intervention.

A few examples highlight our current priorities:

- Cyber risk, mitigated through transfer to the insurance market, is positioned in the "yellow" area due to its potential impact on operational continuity.
- Market risks are distributed across multiple levels, depending on access dynamics, churn rate, and average revenues.

Energy, regulatory, and commercial credit risks carry varying importance depending on the evolution of the external and regulatory context.

We update the matrix periodically, based on forecast data, actual results, and scenario analysis, in order to ensure continuous and responsive oversight. This allows us to anticipate critical issues, strengthen mitigation measures, and optimize the resources deployed in control mechanisms, in line with our risk appetite and our objectives of sustainability, resilience, and long-term value creation.

6. Analysis and Management of the most relevant risks

From the risk matrix in the previous paragraph, we further examine below some of the risks most relevant to the Group, selected based on their positioning, likelihood of occurrence, and the significance of their potential consequences for the business. For each risk, the main exposure factors are described, along with the methodologies adopted for assessment and the related management and mitigation approaches.



Market risks

The evolution of the competitive landscape and of demand, influenced 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-based model (Nash Equilibrium);
- CashFlow@Risk model, focused on the impact on Business Plan targets;
- NPV@Risk model for assessing risks associated with industrial investment projects.

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

- convergent offers with partners such as DAZN, Netflix, and Disney+, which increase perceived value and build customer loyalty;
- continuous improvement of network quality, with investments in infrastructure, including the 5G network;
- targeted acquisition campaigns aimed at customers from other operators;
- monitoring of price/quality positioning, to ensure competitiveness in line with market dynamics.

Energy and climate risks

Energy risk mainly arises from the volatility of energy prices, influenced by the evolving macroeconomic and geopolitical context, and can have significant effects on the Group's operating costs and their predictability.

To assess exposure to this risk, TIM uses a **probabilistic model** that simulates energy price trends, incorporating trends and volatility elements. The methodology for quantifying exposure measures the distance between the 5th percentile of the simulated price and the value forecast in the Plan, making it possible to estimate, on a prudential basis, the potential economic consequences arising from unfavorable energy price movements.



Climate risks include both **physical risks**, arising from the effects of climate change on the Group's infrastructure and operations, and **transition risks**, associated with the evolving regulatory, technological, and market context linked to the shift toward a low-emission economy.

With regard to physical risks, the presence of an extensive and widespread network infrastructure exposes the Group to the effects of climate change and extreme natural events, which can affect asset integrity, operational continuity, and the quality of services provided. The risks considered include both acute events, such as floods, storms, fires, and landslides, and chronic phenomena, such as rising temperatures and heat stress, which can affect infrastructure performance, energy consumption, and related operating costs over time.

The assessment of **physical risks** is based on a structured approach that considers the identification of relevant hazards, asset exposure, and their vulnerability to individual climate events. For acute physical risks, TIM also uses quantitative methodologies to support the estimation of potential economic consequences.

In this context, the **CLIMADA model** makes it possible to assess the potential effects of climate events on assets and to support decisions relating to resilience measures and insurance coverage. These assessments can be supplemented by desk and on-site analyses and by probabilistic simulations of potential direct losses, to identify the most exposed assets and define appropriate prevention and adaptation measures.

TIM is also developing climate analysis tools aimed at assessing future scenarios and medium- to long-term consequences, with the goal of progressively strengthening the integration of climate risks into planning and risk management processes.

With regard to **transition risks**, these arise from the changes associated with the shift toward a low-emission economy and may affect the Group's decarbonization path and the achievement of the climate targets set out in the Transition Plan.

The main risk factors considered relate to:



- the evolution of the regulatory framework and of reporting requirements on climate and sustainability matters, including the possible strengthening of carbon pricing mechanisms;
- growing demand for data traffic, digital services, cloud, and artificial intelligence, with a consequent increase in energy consumption and the need for infrastructure efficiency improvements;
- the evolution and availability of technologies and solutions supporting the energy efficiency of networks and Data Centers, as well as the value chain's ability to contribute to Scope 3 emission reduction targets;
- the evolution of competitive dynamics and the expectations of investors, customers, and other stakeholders regarding the Group's climate commitments and performance.

These factors may lead to economic, financial, and operational consequences, including:

- higher costs and investments related to regulatory and environmental compliance, carbon pricing mechanisms, infrastructure efficiency improvements, and the achievement of decarbonization targets;
- possible deviations from climate targets and the Net Zero trajectory, with potential effects on access to capital and sustainable finance instruments and on the Group's reputation;
- the need to progressively adapt processes, infrastructure, and operating models to respond to technological and market developments and preserve long-term competitiveness.

Energy and climate risk management is integrated into the Enterprise Risk Management processes and consists of mitigation, adaptation, and risk transfer measures, defined according to the different types of exposure.

With regard to energy risk, the Group adopts a policy for managing energy hedging, which involves the use of forward contracts and derivative instruments aimed at limiting the effects of price volatility and stabilizing costs. Exposure is also subject to continuous monitoring, through analyses shared periodically among the functions involved — in particular Planning, Control and Finance, and Procurement — at least on a quarterly basis.



For physical climate risks, exposure and vulnerability analyses of assets support the identification of prevention, adaptation, and resilience measures and, for transferable risks, the definition of risk transfer strategies, including using insurance coverage.

For transition climate risks, the main measures are integrated into the Transition Plan and include:

- maintaining the supply of electricity from renewable sources through Guarantees of Origin, PPAs, and energy self-production initiatives;
- energy efficiency improvements and the modernization of networks, Data Centers, offices, and retail stores;
- the use of innovative technologies and energy monitoring solutions to optimize consumption;
- the progressive electrification of the company fleet and the reduction of fossil fuel use;
- the reduction of emissions along the value chain through the integration of ESG criteria into supplier qualification, selection, and monitoring processes;
- the promotion of circular economy initiatives, and the reuse and refurbishment of equipment and devices.

Across the various risk areas, the Group monitors the evolution of exposures and climate targets through specific KPIs and progressively integrates the results into its decision-making, industrial, and financial processes.

7. Recognition and Management of emerging risks

In continuity with the analysis of the most relevant risks, the Enterprise Risk Management process also considers emerging risks, with the aim of identifying new or evolving phenomena that could have significant consequences for the Group in the medium to long term (3–5 years).



In line with the World Economic Forum model, these risks are characterized by a high degree of uncertainty, difficulty of quantification, and the ability to produce significant changes in the context in which the Group operates.

Risks related to Artificial Intelligence

Within our business context, the adoption of Artificial Intelligence (AI) solutions and systems is steadily growing, in line with the technological evolution transforming the telecommunications sector. TIM uses AI in its own processes and develops and markets solutions based on these technologies, with the aim of generating operational efficiencies, innovating its offering, and responding to evolving customer needs.

However, alongside the growth of AI-related opportunities, new risks are emerging, linked both to the ability to effectively develop and integrate these technologies and to their responsible, secure, and compliant use.

The main risk factors relate to:

- compliance with the regulatory framework, particularly the AI Act, as well as regulations on personal data protection, intellectual property, and copyright;
- the security, quality, and integrity of data and systems, including cybersecurity risks, possible privacy violations, and the need to ensure the reliability of outcomes and prevent algorithmic bias and discrimination;
- the technological and organizational capacity to develop and integrate AI solutions, in terms of availability of specialist skills, interoperability with existing systems, adequacy of infrastructure, and availability of technology supply;
- the economic sustainability of investments, also in relation to the availability of necessary resources, the ability to achieve expected benefits, and the costs of developing, managing, and adapting the solutions;
- transparency and reliability in the use of AI, necessary to preserve the trust of customers, employees, suppliers, and other stakeholders.

The occurrence of these risks may result in economic, legal, and reputational impacts for the Group. The risk of regulatory non-compliance is particularly significant: violation of specific



provisions of the AI Act can result in fines of up to 7% of annual global turnover for the use of prohibited AI systems, and up to 3% for failure to comply with certain requirements applicable to high-risk systems.

In addition, there is the economic risk of not achieving the expected benefits from AI investments, due to revenues or savings falling short of forecasts, or costs for developing, managing, and adapting solutions exceeding expectations.

To manage and mitigate these risks, TIM has established centralized oversight of AI, supported by a cross-functional team involving expertise from Strategy, Finance, Compliance, Legal, Security, and other corporate functions, with the aim of ensuring integrated management across the entire lifecycle of AI systems.

The management model specifically includes:

- a governance framework with defined policies and responsibilities, aimed at regulating the responsible use of AI and promoting a widespread culture of risk awareness;
- the mapping and classification of AI systems, through an up-to-date inventory of the models and solutions in use and risk classification tools consistent with the categories and requirements set out in the AI Act;
- a structured risk management process spanning the entire lifecycle of the solutions, from design to development, testing, and release, following the principles of ethics by design, privacy by design, and security by design;
- post-release monitoring and control activities, including human oversight, periodic performance checks, and prompt identification and correction of any anomalies or bias.

This approach is aimed at ensuring the safe, reliable, and compliant development and use of AI, while safeguarding people, data, and business processes.

IT and security risks

IT risk is linked to the Group's growing dependence on digital technologies, IT infrastructure, and cloud services, resulting in greater exposure to increasingly complex cyber threats. This exposure may be further heightened by the evolving geopolitical and regulatory context, with



potential consequences for service continuity, data security, and the Group's economic and reputational profile.

The evolution of European regulation, including the NIS2 Directive and other cybersecurity-related initiatives, is also strengthening the security and resilience requirements applicable to the telecommunications sector and the resulting compliance obligations.

The main consequences associated with this risk relate to:

- the unavailability or degradation of ICT assets, infrastructure, and services, including as a result of regional infrastructure outages or instability in cloud regions, with particular reference to areas most exposed to geopolitical tensions, such as the MENA region (Middle East and North Africa);
- the compromise of data security and confidentiality, resulting in exposure to penalties in the event of a Data Breach or non-compliance with applicable regulations, including NIS2;
- economic and reputational consequences and loss of customer trust, particularly among institutional and strategic customers, including in the event of cyberattacks linked to geopolitical tensions.

In 2025, no ICT security incidents with a medium or high severity impact occurred; however, five significant incidents were recorded, the consequences of which were contained by existing countermeasures, with no significant financial effects during the period.

IT risk management is based on an integrated system of prevention, monitoring, response, and operational continuity, which includes:

- risk assessment and quantification, through penetration testing, vulnerability assessment, and the use of the FAIR (Factor Analysis of Information Risk) methodology to estimate the potential economic consequences of cyber risks;
- threat monitoring and response, through a Security Operations Center (SOC) active 24/7 and systems for protecting and encrypting sensitive data;
- resilience and operational continuity, supported by ISO 22301 and ISO 27001 certifications, Data Recovery policies, the protection of backups not exposed to public networks, and the integration of supply chain processes into business continuity policies;



- oversight of regulatory compliance, ensured by the Compliance function in coordination with the functions involved in digital processes.

These safeguards enable the Group to monitor the evolution of threats, strengthen its prevention and response capabilities, and contain the potential operational, economic, and reputational consequences associated with cybersecurity events.

Supply chain risks

Geopolitical instability and tensions between major economic systems can create critical issues along the supply chain, increasing pressure on the costs of energy, materials, and labor, as well as on the availability of resources needed for the Group's operations.

While there are currently no direct consequences for TIM Group's business — also considering its limited operational presence in the areas affected by conflicts — a further deterioration of the geopolitical scenario could produce indirect effects on the supply chain and lead to an increase in costs incurred by the Group.

The main consequences considered relate to:

- higher energy costs: regarding the Group's overall economic exposure, as of March 2026 the potential cost increase for 2026 attributable to the conflict between the United States and Iran was estimated at between 3 and 5 million euros, taking into account the open position and colocation, net of Noovle's consumption indexed to the PUN;
- possible disruptions or critical issues in the supply chain, resulting in pressure on the availability and cost of production inputs;
- increases in the cost of materials and labor.

To monitor and contain exposure to these risks, the Group adopts a set of measures including:

- periodic assessment of the energy procurement strategy, involving the Finance and Procurement functions;
- quarterly monitoring of EBITDA@Risk against the Business Plan, in order to assess the potential economic consequences arising from the evolving scenario;



- the use of constrained optimization and statistical regression models to estimate the possible evolution of material and labor costs and support the definition of procurement strategies, including through advance purchases or longer-duration contracts.