Enterprise Risk Management

Issue Brief

ERM Risk Management Model

TIM SA, with the objective of ensuring adequate management of its risks, adopts a structured Enterprise Risk Management (ERM) framework, based on the guidelines of the ISO 31000 standard and the COSO ERM model.

Enterprise Risk Management (ERM) process is a structured, integrated and continuous process that allows the organization to identify potential events that may affect its activities, assess, manage and monitor risks, providing Senior Management with information that aims to support decision-making, through the identification, analysis, assessment and management of the main risks associated with the different business processes, in alignment with the strategic, operational, financial and compliance objectives defined in the Company's Industrial Plan.

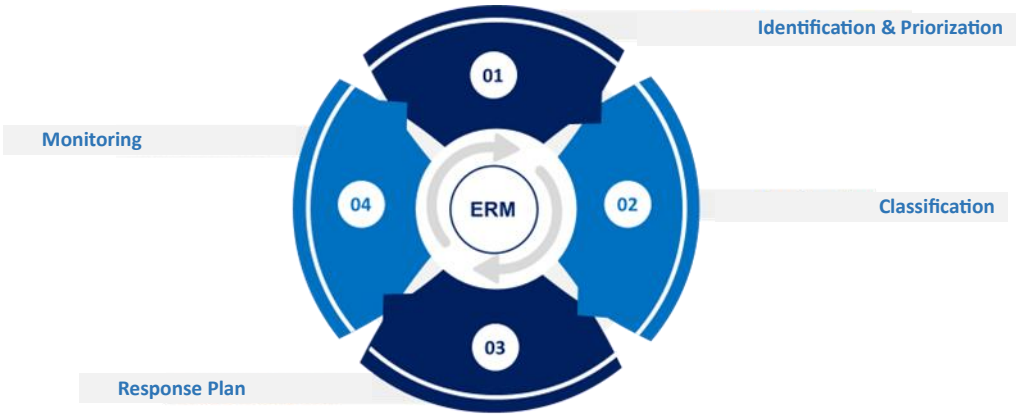
In this context, TIM SA adopted a model that allows for the identification and management of corporate risks in a homogeneous manner, highlighting potential synergies between the functions involved in the company's Internal Controls System, and considering the particularities of each risk scenario.

Therefore, the ERM process aims to effectively manage risks in order to:

- Establish a solid basis for assessing key corporate risks to support the company's decision-making and planning processes;
- Assist the company in managing corporate risks, enabling greater effectiveness in achieving strategic objectives;
- Encourage a proactive approach to corporate risk management;
- Increase the company's awareness of corporate risk management;
- Improve the identification and monitoring of threats and opportunities;
- Improve governance and strengthen stakeholder trust;
- Avoid or reduce losses to the company;
- Prevent or minimize the materialization and possible impacts of corporate risks.

ERM Process

The process is conducted at least **annually** to assess the Company's risk profile and monitor its evolution over time. It is a cyclical process that must be aligned with the Industrial Plan and encompass the following steps:



Identification and Prioritization: This involves identifying internal and external events and factors, including potential emerging risks, that may represent real or potential risks with the potential to negatively impact the company's strategies and objectives. This stage includes reviewing the Corporate Risk Dictionary and prioritizing the risks to be assessed in the current cycle. The main techniques used include:

- Capturing market risks and trends through research into public and external information to TIM (e.g., consulting reports published by consultants and reference organizations, such as the World Economic Forum);
- Capture of risks and sensitivities for the business through interviews with key stakeholders of the company (e.g., executives, members of Committees and Board, Internal Audit, Compliance, among others);

Classification: This consists of assessing the level of exposure of identified and prioritized risks, considering impact and vulnerability criteria. The assessment model for these criteria follows qualitative and quantitative parameters defined in the current methodology and is applied according to the specific characteristics of each risk. The results are compiled and shared with stakeholders, with the support of the Enterprise Risk Management (ERM) team, along with Risk Owners and other risk agents. The risks are then positioned on the Risk Map.

Response Plan: consists of assessing and defining responses to mitigate identified and prioritized risks. During this phase, the Risk Owner , with support from the Risk & Compliance - Enterprise Risk Management department, develops strategies to reduce risk exposure. Possible risk responses include: accept, reduce/mitigate, transfer, or avoid.

Monitoring: This involves continuously monitoring the evolution of risks and response plans. This stage includes overseeing ongoing risk mitigation actions, evaluating the effectiveness of responses, and reviewing risk exposure after the defined measures have been implemented. Throughout the entire cycle, the Risk & Compliance - Enterprise Risk Management area periodically reports on its activities to the Executive Risk Committee, Board of Directors, CAE, and CCR.

Risk Mapping, Classification and Prioritization

In our integrated risk management system, we adopt a structured methodology that begins with a survey of internal and external *inputs, followed by mapping documentation related to risk responses, updating the Risk Dictionary, and prioritizing and validating the risks to be assessed with the Risk* Owners and the Executive Committee. Next, we understand and classify risks, considering impact and vulnerability criteria, as well as identifying the level of governance maturity for mitigation. The results obtained are subsequently validated with the Risk Owners .

At TIM, the **Risk Dictionary** is used to categorize operational risks—those inherent to the business due to their very nature. The various risk events are consolidated and standardized into categories and subcategories, grouping them by related topics.

Currently, the Risk Dictionary is structured into **six main categories** — **Business Model, Financial, Compliance, Resources, Technology and External Events** — and into **15 subcategories** that represent groupings of risks and risk factors with common characteristics, considering their application in the Company's business context: **Customer, Market, Innovation, Strategy, Liquidity, Obligations, Laws and Regulations, Governance, Business Support, Human, Network, IT, Cyber, Catastrophe and Macroeconomics** .

Business Model	Risks related to strategy, operating model and positioning of the company in the market. i.e.: Clients, Market, innovation and Strategy
Financial	Risks that affect financial health and the ability to meet obligations. i.e..: Liquidity and Obligations.
Compliance	Risks related to legal, regulatory, and normative requirements. i.e..: Laws and regulations and Governance.
Resources	Risks involving essential human and operational resources. i.e..: Business and Human Support
Technological	Risks related to technological assets and information security i.e..: Network, IT & Cyber.
External Events	Risks arising from factors external to the company. i.e.: Climate catastrophes and macroeconomics.

Examples of mitigation actions

COMPLIANCE

TIM is subject to Compliance risks arising from any violations of laws, regulations, and internal norms. To mitigate these risks, the Company, among other measures, adopts:

- **Whistleblowing Channel** – availability of a secure, anonymous, and independent channel for registering complaints and reports of non-compliance.
- **Internal and External** Audits – periodic performance of audits to verify adherence to legal, regulatory, and governance requirements.
- **Training** – continuous training of collaborators and leaders on applicable regulatory, ethical, and integrity topics.
- **Compliance and Integrity Policies** – adoption of clear policies, aligned with current legislation and best market practices.
- **Certifications and Recognitions** – maintenance of transparency, anti-corruption, and cybersecurity standards, with certifications such as **ISO 37001**, in addition to the **Pro-Ethics Seal**, and positioning in ESG indices and ratings, such as the **ISE B3**.

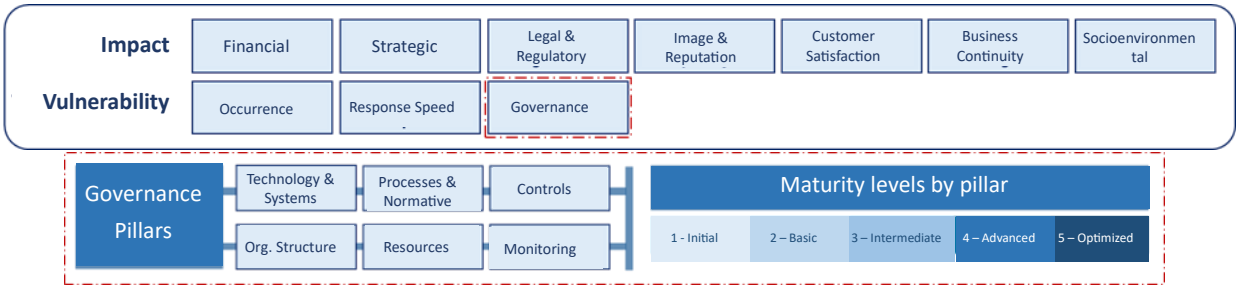
TECHNOLOGY

TIM is subject to Technology risks, arising from failures, unavailability, obsolescence, cyberattacks, or malfunction of systems, networks, and critical infrastructures. To mitigate these risks, the Company, among other measures, adopts:

- **Cybersecurity** – implementation of technologies and controls to prevent, detect, and respond to cyber incidents.
- **Vulnerability Management and Leak Prevention** – continuous monitoring of vulnerabilities, execution of tests and simulations of cyberattacks, and adoption of measures to prevent information leakage.
- **Training** – recurrent training for collaborators on impacts related to legal and regulatory aspects, reinforcing guidelines for data collection, use, treatment, and protection of clients, collaborators, suppliers, and other stakeholders.
- **Certifications** – maintenance of **ISO 27001** certification, which attests to the conformity of the information security management system with international standards.

An example of risks present in our Risk Dictionary is **ESG risk**, related to possible environmental and social impacts on the business and its stakeholders, as well as the inadequate implementation of the Company's guidelines regarding environmental, social and governance issues.

For each category/subcategory mentioned in the table above, a risk assessment and classification are performed, enabling efficient prioritization and resource allocation to mitigate the most critical and/or significant risks to the Company. This classification is based on the Impact and Vulnerability criteria:



The level of risk exposure, both for impact and vulnerability, is analyzed individually based on information obtained in interviews and supported by evidence provided by the Company's areas.

A score from 1 to 4 is awarded according to the level of adequacy in the criterion, the sum of the scores, associated with the weights for each qualifier, results in the final impact and vulnerability score.

The results of our analysis are represented in a risk matrix, as illustrated below. Each risk is ranked according to its level of vulnerability (horizontal axis) and impact (vertical axis) and distributed across four classification levels: Low, Medium, High, and Critical.

This approach allows us to anticipate critical issues, strengthen mitigation measures, and optimize resource allocation within control mechanisms, aligning with our long-term goals of sustainability, resilience, and value creation.

Other actions related to the ERM process

In 2024, we conducted a project to review our corporate risk management methodology, supported by specialized consulting, aiming to strengthen and improve the process. In this context, we conducted training for *Risk Owners* and Risk Agents, focusing on acculturation to the new **Enterprise Risk Management (ERM) model** , and presented the main changes and concepts incorporated into the new methodology to the Committees. As part of this initiative, we published an updated Corporate Risk Management Policy on the intranet, based on market best practices. The main changes were presented to the Committees, and the document was approved by the Board of Directors (CDA) and made available on the Investor Relations website .

Furthermore, to promote and strengthen the corporate risk management culture, **Enterprise Risk Management (ERM) training is available on the corporate intranet** for all company employees. The content presents the concepts, objectives , and steps of the corporate risk

management process, reinforcing the importance of each department's involvement in identifying and mitigating risks.

An internal audit of the risk management process is scheduled for the second half of 2025. Additionally, the company maintains SOx Entity Level control related to Corporate Risk Management, which is subject to annual independent external audits, reinforcing the compliance and robustness of its governance and corporate risk management structure.

TIM approach on Risks Emerging

Risks and Challenges Arising from the Adoption of Artificial Intelligence

Category: Strategic / Technological

Related material topics: Innovation and Technology, Ethics, Integrity and Compliance, Privacy and Data Security

Risk Description: Artificial Intelligence (AI) solutions and systems are increasingly being used across all sectors—including telecommunications—as well as AI applications. While AI solutions offer potential benefits, they also conceal critical issues and ethical pitfalls related to the use of AI that companies, particularly those like the TIM Group, must consider, given their industry and business.

Incorporating AI into company processes brings different challenges and risks that must be considered.

Key challenges from TIM's perspective may include:

- budget availability,
- compliance with laws and regulations,
- data quality, big data and data analysis, real-time decision making,
- technology infrastructure, interoperability and integration with existing systems,
- increased complexity of AI governance and execution.

The main risks (threats) related to the use of AI solutions and systems, to which TIM is potentially exposed, may include:

- breach of compliance with laws and regulations,
- breach of privacy and data security,
- discrimination against individuals/people,
- AI system/output bias,
- cybersecurity.

The potential effects related to the identified risk factors have significant economic, legal and reputational impacts on the Company.

TIM's goals are to adopt a responsible and ethical approach to Artificial Intelligence, accelerate the innovation that can be unleashed by AI, maximize the return on investment in AI opportunities and solutions, and minimize the risks associated with it.

Associated emerging risks: *Adverse outcomes of AI technologies, Disinformation and Cyber Insecurity.*

Impact: The first type of impact for TIM is related to potential non-compliance with the EU AI Act and other future regulations in Brazil. National competent authorities will have enforcement powers with the ability to impose significant financial penalties depending on the level of non-compliance with the AI Act . In Europe, for the use of prohibited AI systems, fines can be up to 7% of the Company's total worldwide annual turnover (revenue) for the previous fiscal year, while non-compliance with the requirements for high-risk AI systems will be subject to fines of up to 3%.

In addition to the compliance impact, a different type of impact for TIM is a potential failure to achieve the overall expected benefits of AI investments, due to, for example, lower revenues generated by AI solutions or higher costs incurred for the development and management of AI solutions.

Management Considerations (Mitigating Actions): We chose to adopt a centralized AI governance model, aligned with the objectives of our Strategic Plan. We established a cross-functional team, composed of experts from various corporate functions (e.g., Strategy, Finance, Compliance, Legal, Security, etc.), to ensure integrated AI management, considering its technical and organizational complexity. Additionally, in 2023, TIM established an Artificial Intelligence Committee, with the objectives of:

- define the company's strategies, policies and procedures to accelerate the responsible adoption of artificial intelligence based on business priorities, involving customers, suppliers and employees;
- identify use cases, in alignment with their respective leaders, through the *test & learn* framework *and subsequent industrialization* ;
- ensure the choice of infrastructure solutions and partner suppliers for the development of use cases;
- enhance the business value of these initiatives through responsible, agile, synergistic management aligned with the company's strategic plan.

This is in view of the following main points:

- The complexity of implementing AI technologies in the business processes involved, employing resources efficiently and effectively to transform AI-enabled opportunities into measurable value generation (e.g., increased productivity, cost optimization) and from a sustainability perspective.

- The contextual need for accountability and protection that requires choosing an integrated (enterprise-level) approach to managing 'emerging' risks related to the use of AI.

In 2024, TIM revised its Code of Ethics and Conduct, establishing the following principles for the responsible use of AI:

- We promote the ethical and responsible use of available technologies, avoiding the development or application of solutions that may cause harm, discrimination, manipulation or improper or unlawful processing of personal data that may cause harm to the individual and their privacy or invasion of privacy.
- We are committed to ensuring that technology is used responsibly, paying attention to the technological control environment, level of governance, and in compliance with applicable standards, following best practices and guidelines adopted nationally and internationally.
- We are committed to developing AI that avoids any type of unlawful discriminatory bias and potential harm that may arise from its use.
- We reaffirm our commitment to using artificial intelligence consciously, always seeking the benefit of society, without compromising our fundamental values.

Cyber Threat Risks and Impacts Linked to the Geopolitical Context

Category: Strategic / Geopolitical / Technological

Related material topics: Privacy and Data Security, Ethics, Integrity and Compliance, Quality of Services, and Innovation and Technology

Risk Description: In today's digital world, cyber risk, coupled with rising geopolitical tensions, represents one of the most critical challenges for businesses and society, particularly for companies like the TIM Group and the entire telecommunications sector. The growing dependence on information technology and the resulting increased interconnectedness of societies have increased vulnerabilities, particularly to cyber threats. The World Economic Forum considers cross-border cyberattacks an area where risk mitigation is still in the early stages of development. TIM's cybersecurity approach is closely aligned with the European Union's strategic objectives. The EU prioritized increasing cybersecurity resilience in critical sectors, including through legislative measures such as the Directive on Security of Network and Information Systems (NIS Directive and on regulatory developments) and the Cybersecurity Law. By implementing robust risk assessment models and sharing best practices with other entities within its group, TIM contributes to broader efforts to strengthen cybersecurity across all its areas of operation. These efforts are crucial to protecting digital infrastructure and promoting a secure digital environment in line with European cybersecurity policies and objectives. Cyberattacks can cause significant damage, not only in terms of direct financial losses but also in terms of reputation and trust. To effectively address these risks, TIM has chosen to take a proactive approach to assessing and subsequently managing cyber risk. Timely risk assessment allows for the identification of vulnerabilities associated with corporate assets and an understanding of the extent of potential threats, thus facilitating the definition of appropriate defense strategies.

Associated emerging risks: *Failure of cybersecurity measures, cybercrimes and cyber insecurity*.

Cybersecurity infrastructure and protection measures may be overwhelmed or rendered obsolete by increasingly sophisticated and frequent cybercrimes.

The company's operations and business are intrinsically linked to the transmission of information and the digital environment. In the context of widespread dependence on increasingly complex digital systems, growing cyber threats are outpacing societies' ability to prevent and effectively manage them.

Cyberattacks are external to the company and can have varied origins and can affect the company , its business and its customers in different ways: resulting from political tensions (access to systems for the transmission of political information, or to harm political movements), sociopolitical movements (such as the intention to invade to gain access to specific data, to

weaken companies in the telecommunications sector or even transmit messages through the company's systems) or even as an indirect consequence of macroeconomic risks (such as the deterioration of economic conditions in the country that lead more people to seek ways to profit illicitly, including the sale or exploitation of data for fraud and cybercrime).

The risk and impacts are specific to the company, as a telecommunications company, our systems are particularly important for operationalizing attacks, and our customer databases comprise a significant portion of people. The company is improving ways to prevent the risk from materializing and mitigate impacts.

Taking a long-term view, we analyze that there are aspects of the LGPD (General Data Protection Law) that will come into effect, but it is still unclear how the ANPD (National Data Protection Authority) will apply fines for data processing violations. There are no precedents or guidelines like those developed by the European Data Protection Board. Therefore, this is an emerging risk, as the Brazilian data protection authority is still establishing its rules, and fines are expected to be imposed. In the absence of dosimetry standards, uneven enforcement may occur.

Impact: The impact of a cyberattack, in addition to damaging the company's reputation, would compromise TIM's business, leading to a lack of trust among strategic customers whose priority is the protection of their data and associated services. Hence the need for a methodology to detect and quantify the risk associated with all possible scenarios, including those arising from potential ongoing geopolitical tensions.

Possible impacts: a) Lack of availability of assets to support the provision of ICT services; b) Penalties for Data Breach; c) Sanctions for non-compliance with the new legislation (NIS 2); d) Loss of trust resulting in loss of customers; e) Reputational damage in the event of geopolitical attacks on institutional customers.

Management Considerations (Mitigating Actions): TIM conducts its cybersecurity activities based on ISO 27001/2013—an international standard that describes best practices for information security management—and NIST (Cyber Security Framework) to support management and reduce information security risks. In this process, since 2017, TIM has implemented protection tools and mechanisms to prevent cyberattacks, offering low-cost solutions and products to improve data protection for our customers and other businesses.

To this end, TIM continually improves its Network Access Filtering, adopts Anti-DDOS, has a threat intelligence service, conducts ongoing vulnerability scans at scale, uses a Responsible Disclosure Platform (Bug Bounty), and has implemented control procedures and invested in prevention, incident handling, and monitoring teams. We are using CIS Controls (Centre for Internet Security Controls) to implement best practices for organizing cybersecurity measures.

TIM conducts independent testing of functions at the second level of control (Technological Compliance). In 2023, TIM began offering its customers, in partnership with EXA Segurança, protection services for banking transactions carried out under duress or resulting from cyber fraud.

At the corporate level, there is an ESG plan goal, seeking for the company to maintain its ISO 27001 certification, which was obtained in 2022. Furthermore, TIM's compliance area continuously monitors regulatory compliance, in line with other functions involved in digital processes.

Cybersecurity processes are increasingly strengthened, consolidated, and managed, supported by the most modern solutions to ensure the best security protection, with preventive monitoring and response actions to minimize the impact on TIM customers.

Other risk management processes

Every two years, we conduct a review of our dual materiality assessment, which involves identifying the company's socio-environmental and financial impacts. In 2024, the ERM department was involved in the dual materiality process, and the ERM risk map was used to identify material issues, thus integrating processes.

Additionally, TIM engages a service provider, periodically and on demand, to assess network, infrastructure and application vulnerabilities with a specialized tool, as well as to simulate EHT - Ethical attacks. Hacking Test. Identified vulnerabilities are classified according to the level of risk they pose to assets and the environment. This is part of the vulnerability assessment process, aiming to ensure ongoing maintenance.

After identification, reports are issued detailing the identified vulnerabilities and forwarded to TIM's CSOC (Cyber Security Operations Center) team, which then contacts those responsible for the assets, including applications, infrastructure, APIs, routers, switches, and integrations, among others. Finally, KPIs are generated based on the volume of tests for vulnerability assessment and EHT penetration tests, to be conducted monthly. Controls are implemented to monitor the achievement of the defined KPI targets. If these targets are not met, the reasons and explanations for achieving these targets are recorded.

It is worth noting that in 2024 TIM revised its operational vulnerability management technologies, integrating the internationally recognized Qualys reference tool : Enterprise Cyber Risk & Security Platform.