CYBERSECURITY

Insight

TIM Group

June 2025

INDEX

1. Cybersecurity at the heart of our commitment to a reliable and secure digital future

We are the leading telecommunications operator in Italy and among the leaders in Europe. This position gives us a unique perspective on cyber threats. Every day, we monitor and analyze hundreds of events to prevent or contain attacks, working tirelessly to protect the TIM Group's network infrastructure, data centers, cloud platforms, and digital services—and, of course, those of our customers.

Within our organization, specialized and coordinated entities operate, such as network security teams, Cyber Security Operations Centers (Cyber SOC), and companies like Telsy. This ecosystem enables us to closely observe the evolution of threats that indiscriminately target citizens, businesses, and institutions.

We also track developments in the regulatory and institutional landscape on cybersecurity to understand how defenses are being strengthened and which measures are being introduced at the European and national levels to enhance prevention and response capabilities against increasingly intense attacks.

We believe in a digital world that is both reliable and secure. That is why we are committed to fostering a true culture of cybersecurity—accessible even to non-experts. For this reason, in 2025 we published the Cyber Security Report 2024 in collaboration with the Cyber Security Foundation, the first Italian non-profit foundation dedicated to the cyber domain.

2. Our Cybersecurity Governance System

To ensure the protection of our infrastructures and the data we process from cybersecurity-related risks, we operate through a structured and coherent governance system.

The Board of Directors holds responsibility for strategic guidance and oversight, including internal control and risk management. In this capacity, it defines the guidelines of the

Internal Control System, verifying its adequacy, effectiveness, and proper functioning to ensure that the company's main risks—including those related to cybersecurity and data protection—are correctly identified, assessed, and managed over time. To this end, the Enterprise Risk Management model we have adopted enables the consistent identification, evaluation, and management of risks across the Group.

At the overall governance level, in carrying out its responsibilities of strategic guidance and oversight—covering internal control and risk management matters—the Board of Directors (BoD) of TIM has established an internal committee focused on controls and risks (the Control and Risk Committee).

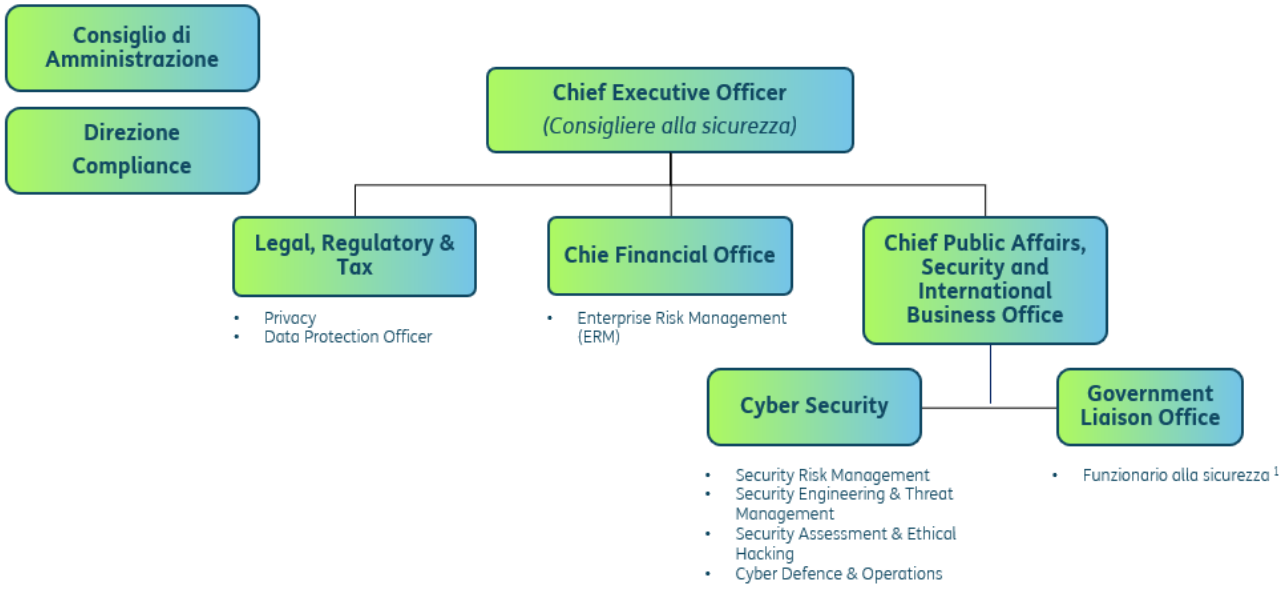
The Control and Risk Committee is an intra-board body composed exclusively of independent directors. It performs preparatory functions to support the Board in its assessments and decisions concerning the risk control and management system, reporting regularly on its activities. Its remit also includes risks related to Cybersecurity and Privacy, areas in which the Committee's Chair brings extensive operational expertise.

The Chief Executive Officer (CEO), in line with the guidelines set by the Board of Directors, is responsible for establishing and ensuring the proper functioning of the internal control and risk management system. The CEO also oversees governance in the areas of Information Security and Cybersecurity, including the management of related risks.

By delegation of the Board of Directors and with the approval of the Government Authority, the CEO holds exclusive authority as the Director for Security Organization, as provided under the Golden Power regulations. This framework requires close cooperation with the Government on matters concerning the security of strategic communication infrastructures and mandates the strengthening of internal security safeguards.

In governing Information Security and Cybersecurity, the CEO relies on the following structures:

- The Chief Public Affairs & Security Officer (CPASO) is responsible for Physical and Cyber Security across the TIM Group. Through the organizational units within his Department—which include Cyber Security and the Security Officer (FAS)—he ensures comprehensive oversight of security matters, in line with the Golden Power regulations and under delegation from the Board of Directors. The CPASO serves as the single point of contact for all security-related issues, supervises measures for the prevention and mitigation of cyber risks, reports directly to the Chief Executive Officer, briefs the Control and Risk Committee, and acts as the liaison with Institutional Authorities.
- The Cyber Security structure, within the Public Affairs & Security Office Department, is organized into the following functions: Security Risk Management, Security Engineering & Threat Management, Security Assessment & Ethical Hacking, and Cyber Defence & Operations.
- The Enterprise Risk Management (ERM) function, within the Chief Financial Office Department, plays a central role in assessing and monitoring corporate risks, including those related to cybersecurity. In this context, ERM periodically receives from the ICT Risk Management function the results of cyber risk analyses, which serve as a key input for the risk quantification model based on the FAIR (Factor Analysis of Information Risk) methodology. This internationally recognized approach makes it possible to estimate, in economic terms, the potential impact of cyber threats and vulnerabilities, translating risk into understandable and comparable metrics. The updated risk profile, developed by ERM using these inputs, not only supports the internal control system but is also directly integrated into the industrial planning process.



(1) The Security Officer in charge of this function is responsible for activities related to the Security Organisation pursuant to the Prime Ministerial Decree of 16 October 2017 and the Golden Power regulations, with full economic and managerial autonomy, and reports directly to the Chief Executive Officer.

Within our governance model, the management of ICT compliance and personal data protection is entrusted to specialized functions that operate in a coordinated manner within the corporate control system, in compliance with applicable regulations and international best practices.

In particular, we adopt the principle of role segregation, which clearly distinguishes operational activities—carried out by the technological functions reporting hierarchically to the Chief Executive Officer—from control activities, entrusted to the Compliance Department. The latter has central responsibility for providing guidance and oversight to the top management and corporate bodies regarding regulatory compliance and the monitoring of corporate implementation procedures. The annual activity plan of the Compliance Department is submitted for approval by the Board of Directors.

Alongside the Compliance Department operates the Data Protection Officer (DPO), an independent role established under EU Regulation 2016/679 (GDPR). The DPO is responsible for overseeing the protection of personal data processed by TIM and the Group companies.

Reporting directly to the Data Protection Authority, the DPO supervises compliance with data protection legislation. The DPO's activities are supported by the Privacy Control Plan, carried out by the Compliance Department as part of its annual plan.

3. The National Cybersecurity Governance System

In addition to our governance structure dedicated to cybersecurity, as a strategic operator for the Country, we are subject to a complex national and European regulatory framework that covers both the security of critical infrastructures and the protection of data and privacy.

The Golden Power decrees, introduced in 2017, establish specific obligations for companies operating in strategic sectors such as telecommunications. In particular, we are required to:

- adopt dedicated security and control measures;
- provide periodic reports to the Government Authority on the implementation of these measures.

Decree-Law 21/2022, enacted in response to the Ukrainian crisis, further strengthened the special powers of the Presidency of the Council of Ministers and introduced stricter rules for 5G networks, considered critical infrastructures for national security.

Our commitment to security is also institutionally recognized. The implementation of the measures required by law is subject to verification by a Monitoring Committee established at the Presidency of the Council of Ministers, tasked with overseeing compliance with regulatory obligations and, where necessary, imposing sanctions. The activities carried out by this Committee have confirmed that TIM maintains high security standards, achieved through the cross-functional involvement of various corporate Departments and coordinated by the Chief Public Affairs & Security Office, which ensures the effective implementation of measures to safeguard national interests. Since 2021, the regulatory framework has been further reinforced with the implementation of Law 133/2019, which established the National Cybersecurity Perimeter (Perimetro di Sicurezza Nazionale Cibernetica – PSNC). This set of rules aims to ensure a high level of protection for operators

managing ICT services essential to national security, including TIM, which is formally registered within the Perimeter.

Finally, the new Directive 2022/2555 (NIS2), which replaces the current Directive 2016/1148 (NIS), entered into force on 16 January 2023 and was transposed into national legislation by 17 October 2024, becoming applicable from 18 October 2024.

NIS2 broadens the scope of rules on the security of networks and information systems. On the one hand, it incorporates sectors currently covered by other regulations, which are simultaneously repealed (e.g. network and electronic communications service security measures currently included in the European Electronic Communications Code); on the other, it extends the rules to new entities (e.g. data centers, CDNs, etc.).

The Directive maintains the obligation to adopt risk-based security measures but introduces a series of minimum baseline requirements, including supply chain security management, and revises the procedures for mandatory reporting of cybersecurity incidents.

Penalties for non-compliance can reach up to 2% of annual revenue.

The Directive also strengthens supervisory bodies and activities at the EU level, aiming to improve collaboration against global cyber threats through information-sharing among member states.

Within this framework, the National Cybersecurity Agency (ACN) has been established to oversee, coordinate, and enhance Italy's resilience to the increasingly complex and pervasive evolution of cyber threats.

Our collaboration with institutions on cybersecurity matters is constant and structured. We actively participate in numerous working groups within institutional bodies, including the Prime Minister's Office, the Ministry of the Interior, and the Ministry of Defence, through the involvement of our specialized cybersecurity teams.

4. Information security policy

The Information Security Policy applies to all functions within the TIM Group and pursues the following objectives:

- define the Group's information security objectives;
- TIM Group's commitment, through its management, to meeting information security requirements within a process of continuous improvement;
- set out the information security requirements the TIM Group intends to adopt.

This Policy extends to all corporate assets (processes and technologies) that handle information on behalf of the TIM Group. It also applies to the entire workforce, whereby each function—and therefore every individual within it—shares responsibility for achieving the objectives defined in the Policy through the adoption and implementation of specific actions.

Through the adoption of this Policy, TIM Group undertakes, among other things, to:

- define processes, roles, and responsibilities for information security;
- ensure a level of confidentiality, integrity, protection, and availability of information proportionate to its business value, i.e., to the direct or indirect losses that a security incident may cause to the services provided to its customers;
- raise awareness and provide training for staff on information security;
- monitor, analyze, and respond to any incident—or suspected incident—affecting information security;
- define cybersecurity requirements for external parties (e.g., suppliers). Contracts and agreements with Third Parties must include requirements and clauses to ensure the protection of TIM Group's information and intellectual property, compliance with applicable regulations, adequacy of the skills of the personnel involved, security levels consistent with corporate policies, monitoring and control tools (including continuity and

incident management plans), audit rights for TIM, as well as service levels and penalties aligned with—or stricter than—those applied to the Group's customers;

- cooperate with Institutions and Authorities to share methodologies and best practices aimed at the continuous improvement of its security policies and, consequently, of its information security systems, in order to protect and create value for the Group.

5. Information Security Policy Management Programs

To achieve the objectives defined in the policy, TIM has established an Information Security Management System (ISMS) designed to ensure governance of the processes and activities specific to the security of the Information assets. This system includes:

- the introduction of a business continuity plan related to cybersecurity, which is part of the broader business continuity management system adopted by the Group to safeguard the operation of its critical processes at an adequate level in the event of incidents that could compromise service delivery. This plan consists of a set of procedures that enable the prevention of potential threats, limit and mitigate possible damage, and restore the process;
- the detection, analysis, and proper management of cybersecurity vulnerabilities to prevent and reduce security incidents;
- the conduct of assessments of the IT infrastructure aimed at evaluating its adequacy against the company's regulatory framework, applicable mandatory regulations, adopted standards, and implemented security requirements;
- the performance of third-party audits and assessments of the Information Security Management System. In this regard, it should be noted that the Group has obtained ISO 27001 certification (valid until 06/12/2026);

- the delivery of training courses, available to all TIM Group personnel, aimed at increasing their awareness of information security;
- the definition and consequent activation of an escalation process for reports related to incidents, vulnerabilities, or suspicious activities received from TIM Group personnel, which are taken in charge and managed by the IT and Crisis Management function.

During 2024, a total of 16 events were confirmed, classified as IT incidents or breaches.