INFORMATION SECURITY AND CYBERSECURITY GOVERNANCE

TIM

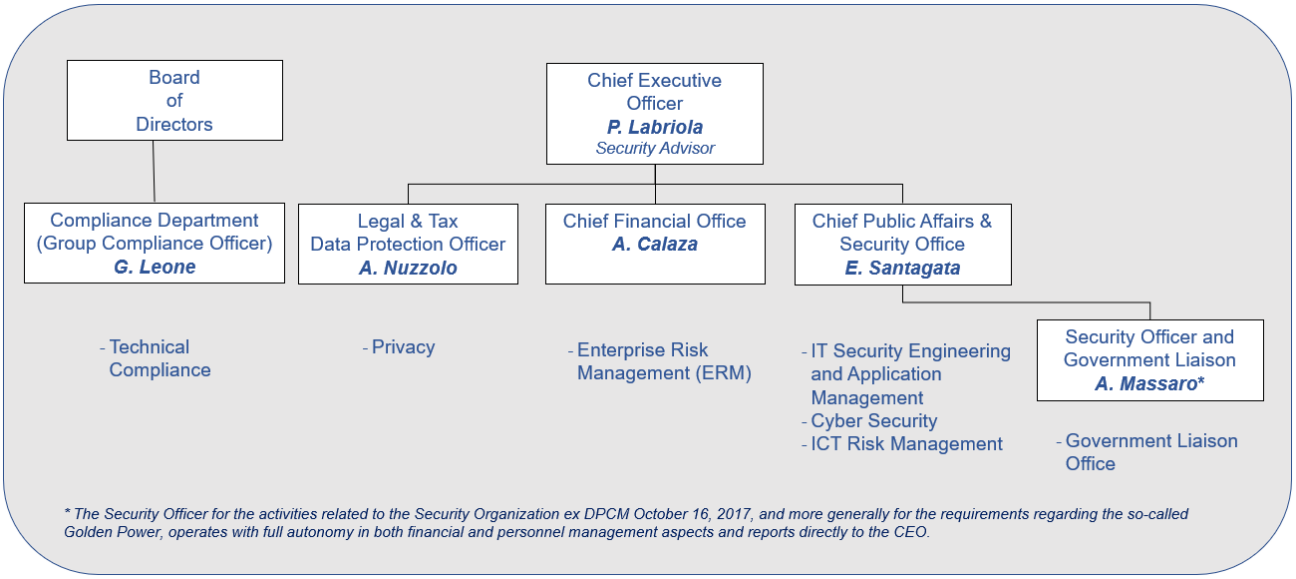
June 2023

Electronic communication services are based on ICT technologies and are therefore essential to business, government, garrison and counter cybersecurity risks. Infrastructure security, data protection and continuity of services provided are priorities for every telecommunications operator, and certainly they are for TIM, whose infrastructure has historically been the backbone of the country's communications system and is proposed as a major national player for datacenter and cloud services for public and private customers.

At the overall level of governance, in the fulfilment of its responsibilities of strategic direction and supervision, extended to the issues of control and risk management, the Board of Directors (Board of Directors) TIM organized itself by setting up an internal committee focused on controls and risks (the Control and Risk Committee).

Notwithstanding the delegation to the Chief Executive Officer (as such, also responsible for the establishment and maintenance of the internal control and risk management system, is hereby terminated, in accordance with the guidelines given by the Council plenum)The Board of Directors has kept the hierarchical oversight directed on a function focused also on the control of the conformity of technological processes and IT security (Compliance Management, through the Technical Compliance structure). More generally, reporting directly to the CEO, the TIM Group oversees the themes of Information Security and Cybersecurity Governance and manages the associated risks not only in widespread and transversal terms, but using dedicated processes and structures such as:

- in the **Public Affairs & Security Office** through the organizational structures: **Cyber Security**, **ICT Risk Management, IT Security Engineering and Application Management** and that related to the Security Officer and Government Liaison
- in **Legal & Tax** through the organizational structure **Privacy** and the **Data Protection Officer**
- Within the **Chief Financial Office** through the **Enterprise Risk Management** (ERM) structure.



Upstream of these choices lie the specificities peculiar to the Industry, independently assessed by TIM, but also an articulated regulatory framework of national and EU enactment, relating both to infrastructure security and to the protection of data processing and privacy.
These are precepts of general application, but also a special discipline, which subjects the TIM

Group to extraordinary requirements, as it is engaged in the performance of activities of strategic importance for the country either, in general, with respect to communication services, or for defense and national security. The so-called Golden Power decrees, issued in 2017, entailed the imposition of specific prescriptions/conditions and burdened the TIM Group with punctual fulfillments, with the obligation to report periodically to the Government Authority on the status of implementation of the prescribed measures. In addition, the recently published Decree-Law No. 21 of March 21, 2022 (Urgent measures to counter the economic and humanitarian effects of the Ukrainian crisis) strengthened the discipline of the special powers of the Prime Minister's Office in the field of critical infrastructure, in light of the increased strategic nature of certain sectors. Among the measures introduced is the revision of the discipline of special powers pertaining to broadband electronic telecommunication networks with 5G technology.

The robustness of the organizational solutions and the high security standards in place have thus been recognized at the institutional level. On the other hand, the presence of a context of specific rules, subject to control by a special Monitoring Committee at the Presidency of the Council of Ministers, has accentuated-if possible-awareness and attention in the cybersecurity perimeter, entailing an important reorganization of the subject and of the related oversight.
As of 2021, the regulatory framework is enriched by the implementing decrees of Law 133/2019, which defines the Cybersecurity National Perimeter (PSNC). In this context, moreover, the National Cyber Security Agency is established, with oversight tasks to guard the dimension of resilience to the evolution of the cyber threat in its many forms, an evolution that requires further raising the level of security for ICT services essential for National Security purposes, for which TIM is enrolled in the PSNC.

In summary, the governance of cybersecurity issues is broken down as follows:

- **TIM's Board of Directors** defines the guidelines of the Internal Control System, verifying its adequacy, effectiveness and proper functioning, so that the main business risks are correctly identified and managed over time. To this end, the Enterprise Risk Management model adopted makes it possible to identify, assess and manage risks uniformly within the Group. Particular focus is placed on the relationship between the ERM process and the industrial planning process within which the relevant indicators to be monitored associated with the different categories of business plan objectives are identified. Specifically in Information Security and Cyber Security, the ICT Logical Security indicator is constantly monitored by the ERM function, which measures the degree of coverage of the ICT Risk Management process. The ERM function is organizationally located in the Chief Financial Officer Department.
- The Board of Directors of the TIM Group establishes an internal **Control and Risk Committee,** currently made up of only independent directors, with the function of providing preparatory support to the full Board with respect to the assessments and determinations of competence relating to the Internal Control and Risk Management System. The Committee meets according to its own annual schedule and, as a rule, to precede the meetings of the Board of Directors, to which it reports from time to time on its activities. The risks under consideration by the Audit and Risk Committee frequently include cybersecurity risks and measures to protect Privacy.

- In order to better respond to regulatory requirements and to be aligned with international best practices, the **organizational model for ICT compliance** oversight applies the principle of

segregation of duties between operational responsibilities, assigned to the Functions that implement technological processes (which report hierarchically to the Chief Executive Officer) and the central responsibility for control and reporting to Top Management and Corporate Bodies, assigned to the Compliance Department (which reports hierarchically to the Board of Directors), with a guiding responsibility for the purposes of compliance with reference regulations and subsequent monitoring of corporate implementation procedures. The Compliance Department's Annual Plan of Activities is submitted to the Board of Directors for approval.

- The **Data Protection Officer (DPO),** performs the function of directing and supervising the protection of personal data processed by TIM and Group Companies, as required by the EU Regulation 2016/679 (General Data Protection Regulation, GDPR) and liaises with the national authority, the Data Protection Authority. The Data Protection Officer's task of overseeing compliance with personal data processing regulations is ensured by the plan of control activities for privacy compliance purposes executed by the Compliance Department as part of its Annual Plan.

- In order to strengthen the framework of close cooperation with the Government with respect to the issues of security of strategic communication infrastructures, the **Golden Power discipline** requires - among other things - the strengthening of internal security safeguards, to be implemented through the exclusive delegation to a Director on the Security Organization and its involvement in corporate governance with particular reference to all decision-making processes pertaining to strategic activities and the network. With the consent of the Governing Authority, the Board of Directors assigned this delegation to the Chief Executive Officer and identified the Security Officer, who coordinates the Security Organization, in the Head of the Security Function, who in this way is the single point of contact for both Physical and Cyber security issues. In order to monitor the compliance activities carried out by the TIM Group, a special Monitoring Committee is established at the Prime Minister's Office with the task of verifying compliance with the requirements imposed by the decree and imposing possible sanctions in case of non-compliance. The verification action by the aforementioned Monitoring Committee has confirmed the implementation in TIM of high security standards, with the transversal involvement of the various corporate Functions and with intervention tools prepared by the Security Function of the TIM Group to ensure the framework of direction and control of the activities legislatively provided for to guard the corporate perimeters for the interests of national defense and security. The collaboration ensured to the Institutions by the TIM Group in cybersecurity matters is constant and fruitful, and proof of this are the numerous activities carried out within various Working Groups at various Institutional Bodies in which TIM Security - with the Cyber Security Functions - is present (e.g., Technical Tables at the Presidency of the Council of Ministers, Ministry of the Interior and Ministry of Defense).
- The **Security Officer** is responsible for supervising and following up on the activities inherent in the application of measures to counter cybersecurity risks on the Company's perimeter of responsibility. He reports to the Chief Executive Officer and routinely reports to the Audit and Risk Committee, as well as being the contact person to the Institutional Bodies. To ensure cybersecurity oversight, he relies on:
    - specific processes, aligned with international best practices, for prevention (i.e.: ICT Risk Management) and reaction (i.e.: Monitoring and management of information security incidents). Specifically, the ICT Risk Management process aims to reduce cyber

risk by ensuring-through a process of threat analysis, identification of vulnerabilities and definition of countermeasures in prevention-the confidentiality, integrity and availability of processed information. This action enables the Company to assess information security needs in the context of business objectives, as well as regulatory compliance measures in accordance with the Compliance Department. The development of the process is declined internally within the TIM Group by means of appropriate organizational procedure "ICT Risk Management" and provides under the supervision of the Security Officer, with a view to Shared Responsibility, the involvement of all functions, technological and non-technological, which have operational responsibilities and oversee the business processes involved.

To recap, the figures involved, and their CVs are:

- **Pietro Labriola, Chief Executive Officer, General Manager and Security Advisor.** https://www.gruppotim.it/it/gruppo/organizzazione/amministratore- delegato.html
- **Federico Ferro Luzzi, Chairman Risk Control Committee** https://www.gruppotim.it/it/gruppo/governance/comitati/comitato-controllo-e-rischi.html
- **Eugenio Santagata, Chief Public Affairs & Security Office** https://www.gruppotim.it/it/archivio-stampa/corporate/2022/CS-TIM-Nomina-Santagata.html
- **Adrian Calaza, Chief Financial Officer** https://www.gruppotim.it/content/dam/gt/sostenibilità/doc-varie/2022/CV- Adrian-Calaza.pdf
- **Giampaolo Leone, Group Compliance Officer e Head Compliance Department** https://www.gruppotim.it/content/dam/gt/sostenibilità/doc-varie/2022/CV-Giampaolo-Leone.pdf
- **Agostino Nuzzolo, Legal & Tax Director and Data Protection Officer** https://www.gruppotim.it/content/dam/gt/sostenibilità/doc-varie/2022/CV- Agostino-Nuzzolo.pdf