TIM

INFORMATION SECURITY AND CYBER-SECURITY

GOVERNANCE

July 2024

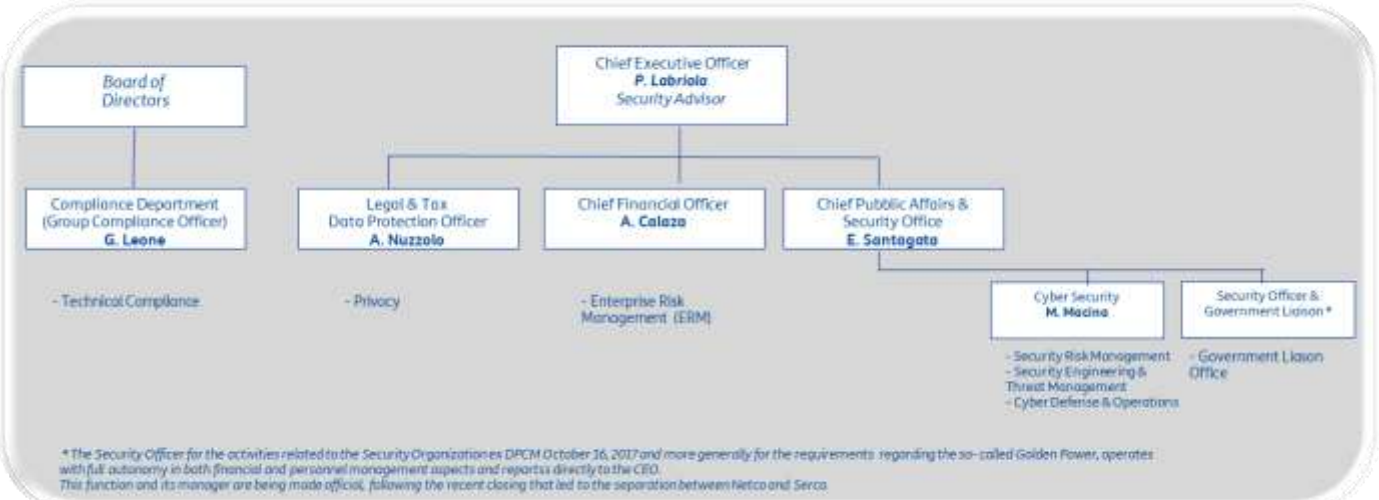
Network infrastructures and data centres form the backbone on which TIM, Italy's leading ICT provider, builds its offer dedicated to households, businesses and the public administration. In order to ensure the cyber-security of its infrastructures and the continuity of the services provided, as well as to guarantee the protection of the data processed, TIM is primarily committed to preventing and combating cyber-security risks through an adequate governance system.

In fulfilling its responsibilities of strategic guidance and supervision, extended to the issues of control and risk management, TIM's Board of Directors (BoD) has set up a special internal board committee focused on risk control (Control and Risk Committee) on an overall governance level.

Without prejudice to the delegation of powers to the Chief Executive Officer (who is also responsible for setting up and maintaining the internal control and risk management system, based on the guidelines issued by the plenum of the Board of Directors) and in accordance with the hierarchy of control measures adopted at TIM Group level, the Board of Directors has identified the direct hierarchical super-ordering of a function that also focuses on monitoring the compliance of technological and IT security processes, i.e. the Compliance Department (2nd level of control).

Moreover, reporting directly to the CEO, governance on Information Security and Cyber-Security issues and related risks are managed using dedicated processes and structures as follows:

- As for the **Public Affairs & Security Office**, the **Cyber-Security** organisational structure with reference to its **Security Risk Management, Security Engineering and Threat Management** and **Cyber-Defence & Operations** offices, and the one assigned to the **Security Officer within which the Government Liaison Office is located**.
- As for **Legal & Tax**, the **Privacy** organisational structure **and Data Protection Officer**.
- As for the **Chief Financial Office,** the **Enterprise Risk Management** (ERM) structure.



In addition to the specific governance structure, there is a complex national and EU regulatory framework specific to the industry relating to both infrastructure security and the protection of data processing and privacy.

These are rules of general application, but also a special protocol which subjects TIM Group to extraordinary requirements, as it is engaged in activities of strategic importance for the country both with respect to communication services and for national defence and security. To be specific, the so-called Golden Power decrees issued in 2017 provide for TIM Group to impose specific requirements/conditions and punctual fulfilments, with the obligation to periodically report to the Government Authority on the status of implementation of the prescribed measures. In addition, Decree-Law No. 21 of 21 March 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. The measures introduced involve the revision of the regulation of special powers relating to broadband telecommunications networks with 5G technology.

The robustness of the organisational solutions and the high security standards in place are therefore also recognised at institutional level. The presence of a context of specific rules, which are monitored by a special Monitoring Committee at the Prime Minister's Office, has further heightened awareness and attention in the Cyber-security perimeter, with an important reorganisation of the subject and its supervision. In 2021, the regulatory framework saw the addition of the implementing decrees of Law 133/2019, which defines the Cyber National Security Perimeter (PSNC). The National Cyber-Security Agency was also established with control tasks to guard the resilience to the evolving cyber-threat in its multiple forms, an evolution that requires a further increase in the level of security for ICT services that are essential for National Security, for which TIM is a member of the PSNC.

In summary, the governance of Cyber-Security issues is as follows:

- A **Board of Directors** that defines the guidelines of the Internal Control System verifying its adequacy, effectiveness and proper functioning, so that the main corporate risks are correctly identified and managed over time. To this end, the Enterprise Risk Management model adopted allows risks to be identified, assessed and managed 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 target categories of the business plan are identified. To be specific, ERM periodically receives the results of the analyses made by the ICT Risk Management function, which constitute an input to the Cyber-risk quantification model (FAIR methodology), and, on the basis of this data, returns the updated risk profile. The ERM function is organisationally located within the Chief Financial Officer Department.
- An **Internal Board Committee for Control and Risks**, comprised solely of independent directors, with the function of providing preparatory support to the plenum with respect to evaluations and determinations of competence relating to the Internal Control and Risk Management System. The Committee meets according to an annual schedule that, as a rule, precedes the meetings of the Board of Directors, to which it reports on its activities. Within its area of responsibility, the Board also oversees risks related to cyber security and privacy, and sees in the figure of its Chairman the person with the greatest operational expertise on these issues. In order to better respond to regulatory requirements and be aligned with international best practices, the **organisational model for ICT compliance management** 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).
- A **Compliance Department** with central responsibility towards senior management and corporate bodies for providing guidance and controlling compliance with relevant regulations, as well as monitoring corporate implementation procedures. The Compliance Department's annual activity plan is submitted to the Board of Directors for approval.
  - A **Data Protection Officer (DPO)** who directs and supervises the protection of personal data processed by TIM and Group Companies, as provided for by EU Regulation 2016/679 (General Data Protection Regulation, GDPR) and liaises with the national authority, the *Garante per la protezione dei dati personali.* The Data Protection Officer's task of supervising compliance with the law on the processing of personal data is ensured by the plan of control activities for privacy compliance carried out by the Compliance Department as part of its annual plan.
  - The **Chief Executive Officer** who, upon assignment by the Board of Directors and with the approval of the Government's authority, has the exclusive delegation of Administrator over the Security Organisation in accordance with the Golden Power regulation - which sanctions close cooperation with the Government with respect to the security issues of strategic communication infrastructures - and requires the strengthening of internal security controls, to be implemented through the aforementioned person, who is also involved in corporate governance with particular reference to all decision-making processes pertaining to strategic activities and the network.

- A **Chief Public Affairs & Security Officer (CPASO)** who, through the specific Cyber-security and Physical Security organisational offices and the Security Officer (FAS), ensures the supervision of Information and Cyber-security for TIM Group, consistent with the Golder Power regulation and as assigned by the Board of Directors. The **Chief Public Affairs & Security Officer** is the single point of contact when it comes to both Physical and Cyber-security issues, supervising the activities inherent to the application of measures to counter Cyber-Security risks within the Company's perimeter of responsibility. He/she reports to the Managing Director and reports to the Control and Risk Committee, as well as being the contact person for the Institutional Bodies. In order to ensure Cyber-Security, he/she uses specific processes, aligned to international best practices, for prevention (i.e: ICT Risk Management) and reaction (i.e.: Computer security incident monitoring and management). In particular, **ICT Risk Management** aims to reduce cyber-risks and guarantee the confidentiality, integrity and availability of the information processed, through a process of threat analysis, identification of vulnerabilities and preventive definition of countermeasures. This action enables the company to assess information security needs in the context of business objectives, as well as regulatory compliance measures in agreement with the Compliance Department. The process is governed by a specific 'ICT Risk Management' organisational procedure and, with a view to the principle of *shared responsibility* in addition to the supervision by the Security Officer, provides for the involvement of all the functions that have operational responsibilities and oversee the business processes involved.

In order to monitor the compliance activities carried out by TIM Group, a special Monitoring Committee has been set up at the Prime Minister's Office with the task of verifying compliance with the requirements imposed by the decree and to impose sanctions in the event of non-compliance. The verification action carried out by the aforementioned Monitoring Committee confirmed the implementation of high security standards in TIM, with the transversal involvement of the various corporate Functions and with intervention tools set up by TIM Group's Chief Public Affairs & Security Office to guarantee the framework of direction and control of the activities that are regulated by law in order to safeguard the corporate perimeters in national defence and security interests. The cooperation ensured to Institutions by TIM Group in the field of Cyber-security is constant and profitable, and this is proved by the numerous activities carried out within various Working Groups at various Institutional Bodies where TIM Security is present with the Cyber-Security Functions (e.g. Technical Tables at the Prime Minister's Office, Ministry of the Interior and Ministry of Defence).

Below are the figures involved in the governance process with their CVs:

- Pietro Labriola, Chief Executive Officer, General Manager and Security Advisor.
https://www.gruppotim.it/en/group/organization/chief-executive-officer.html

- Federico Ferro Luzzi, Chairman Risk Control Committee
https://www.gruppotim.it/en/group/governance/committees/control-risk-committee.html

- Eugenio Santagata, Chief Public Affairs & Security Office
https://www.gruppotim.it/en/press-archive/corporate/2022/PR-TIM-Appointment-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 Office
https://www.gruppotim.it/content/dam/gt/sostenibilit%C3%A0/doc-varie/2022/CV-Agostino-Nuzzolo.pdf