GOVERNANCE DELLA SICUREZZA DELL'INFORMAZIONE

E DELLA CYBERSECURITY

TIM

Luglio 2024

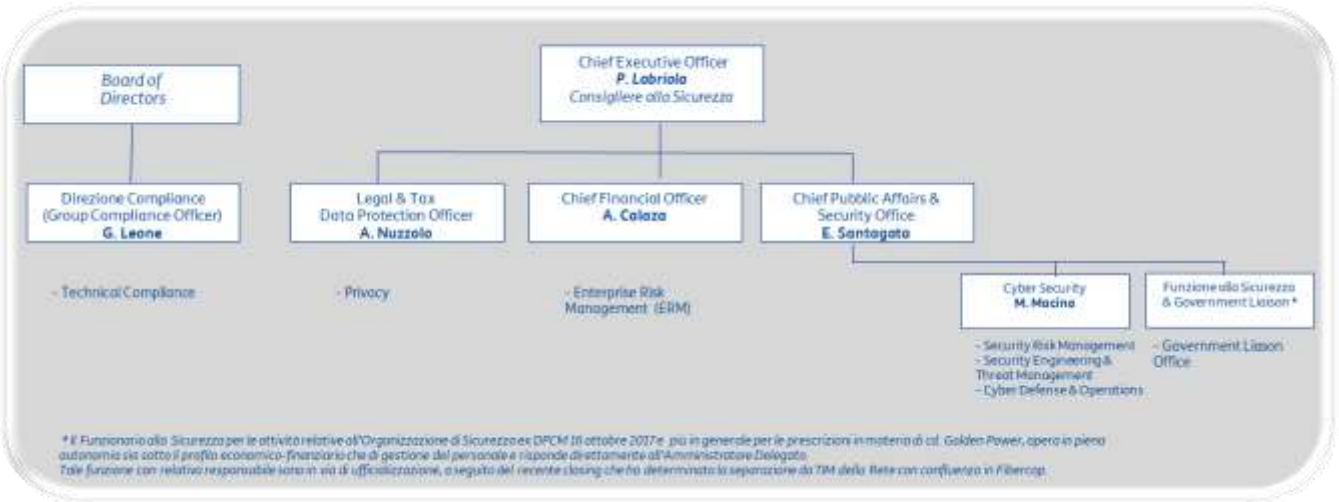
Le infrastrutture di rete e i data center costituiscono l'asse portante su cui TIM, leader in Italia nel settore dell'ICT, costruisce la propria offerta dedicata alle famiglie, alle imprese ed alla pubblica amministrazione. Per assicurare la sicurezza informatica delle proprie infrastrutture e la continuità dei servizi erogati, nonché per garantire la protezione dei relativi dati trattati, TIM è prioritariamente impegnata sulla prevenzione e sul contrasto dei rischi di Cyber Security attraverso un adeguato sistema di governance.

A livello complessivo di governance, nell'espletamento delle proprie responsabilità di indirizzo e supervisione strategica, estese alle tematiche del controllo e della gestione del rischio, il Consiglio di Amministrazione (CdA) di TIM ha istituito un apposito comitato endoconsiliare focalizzato sul controllo dei rischi (Comitato per il controllo e i rischi).

Ferma la delega al Chief Executive Officer (responsabile anche dell'istituzione e del mantenimento del sistema di controllo interno e gestione dei rischi, sulla scorta degli indirizzi impartiti dal plenum consiliare), il CdA ha individuato, secondo la gerarchia dei presidi di controllo adottati a livello di Gruppo TIM, la sovra ordinazione gerarchica diretta su una funzione focalizzata anche sul presidio della conformità dei processi tecnologici e di sicurezza IT, la Direzione Compliance (II° livello di controllo).

Inoltre, a diretto riporto del CEO, la governance sui temi di Information Security e Cyber Security ed i relativi rischi sono gestiti avvalendosi di processi e strutture dedicati quali:

- In ambito **Public Affairs & Security Office** attraverso la struttura organizzativa **Cyber Security,** con riferimento alle sue articolazioni **Security Risk Management, Security Engineering and Threat Management** e **Cyber Defense & Operations,** e attraverso quella assegnata al **Funzionario alla Sicurezza all'interno della quale è prevista la collocazione del Government Liaison Office.**
- In ambito **Legal & Tax** attraverso la struttura organizzativa **Privacy e il Data Protection Officer.**
- In ambito **Chief Financial Office** attraverso la struttura **Enterprise Risk Management** (ERM).



Alla specifica struttura di governance si aggiunge l'articolato quadro normativo nazionale e comunitario, specifico dell'industry relativo sia alla sicurezza delle infrastrutture sia alla protezione dei trattamenti dati e della privacy.

Si tratta di precetti di applicazione generale, ma anche di una disciplina speciale, che assoggetta il Gruppo TIM a prescrizioni straordinarie, in quanto impegnato nello svolgimento di attività di rilevanza strategica per il Paese sia rispetto ai servizi di comunicazione, sia per la difesa e la sicurezza nazionale. Nello specifico, i c.d. decreti Golden Power, emanati nel 2017, prevedono per il Gruppo TIM l'imposizione di specifiche prescrizioni/condizioni e di puntuali adempimenti, con l'obbligo di relazionare periodicamente all'Autorità di Governo sullo stato di attuazione delle misure prescritte. In aggiunta, il D.L. n. 21 del 21 marzo 2022 (Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina) ha rafforzato la disciplina dei poteri speciali della Presidenza del Consiglio in materia di infrastrutture critiche, alla luce

dell'accresciuta strategicità di alcuni settori. Tra le misure introdotte, rientra la revisione della disciplina dei poteri speciali inerenti le reti di telecomunicazione a banda larga con tecnologia 5G.

La robustezza delle soluzioni organizzative e gli elevati standard di sicurezza in essere sono dunque riconosciuti anche a livello istituzionale. La presenza di un contesto di regole specifiche, oggetto di controllo da parte di apposito Comitato di Monitoraggio presso la Presidenza del Consiglio dei Ministri, ha accentuato ulteriormente la consapevolezza e l'attenzione nel perimetro Cyber Security, con un importante riordino della materia e del relativo presidio. A partire dal 2021, il quadro normativo si arricchisce per effetto dei decreti attuativi della Legge 133/2019 che definisce il Perimetro di Sicurezza Nazionale Cibernetica (PSNC). In tale contesto, peraltro, è istituita l'Agenzia per la Cyber sicurezza Nazionale, con compiti di controllo a presidio della dimensione della resilienza all'evolversi della minaccia cibernetica nelle sue molteplici forme, evoluzione che richiede un ulteriore innalzamento del livello di sicurezza per i servizi ICT essenziali ai fini della Sicurezza Nazionale, per i quali TIM è iscritta al PSNC.

In sintesi, la governance dei temi di Cyber Security è così articolato:

- **Consiglio di Amministrazione** che definisce le linee di indirizzo del Sistema di controllo interno, verificandone l'adeguatezza, l'efficacia e il corretto funzionamento, così che i principali rischi aziendali siano correttamente identificati e gestiti nel tempo. A questo scopo il modello di Enterprise Risk Management adottato consente di individuare, valutare e gestire i rischi in modo omogeneo all'interno del Gruppo. Particolare focus è posto sulla relazione tra il processo ERM e il processo di pianificazione industriale all'interno del quale vengono identificati gli indicatori rilevanti da monitorare associati alle diverse categorie di obiettivi del piano industriale. Nello specifico, ERM riceve periodicamente dalla funzione ICT Risk Management le risultanze delle loro analisi che costituiscono un input al modello di quantificazione del rischio Cyber (metodologia FAIR) e, sulla base di questi dati, restituisce il profilo di rischio aggiornato. La funzione ERM si colloca organizzativamente nella Direzione Chief Financial Officer.
- **Comitato endoconsiliare per il controllo e i rischi**, costituito da soli amministratori indipendenti, con funzione di supporto istruttorio del plenum rispetto alle valutazioni e alle determinazioni di competenza relative al Sistema di Controllo Interno e Gestione dei Rischi. Il Comitato si riunisce secondo un calendario annuale che, di regola, precede le riunioni del Consiglio di Amministrazione, a cui riferisce delle attività svolte. Nell'ambito dei rischi di competenza, l'Organo supervisiona anche quelli legati a Cyber Security e alla privacy, e vede nella figura del proprio Presidente la persona con le maggiori competenze operative su tali temi.Al fine di meglio rispondere alle prescrizioni normative e di essere allineati alle best practice internazionali, il **modello organizzativo per il presidio della compliance ICT** applica il principio della segregation of duties tra le responsabilità operative, assegnate alle Funzioni che attuano i processi tecnologici (che rispondono gerarchicamente al Chief Executive Officer).
- **Direzione Compliance** con responsabilità centrale di indirizzo e di controllo verso il vertice e gli organi societari della conformità delle normative di riferimento e del monitoraggio delle procedure aziendali di attuazione. Il Piano annuale delle attività della Direzione Compliance è sottoposto all'approvazione del Consiglio di Amministrazione.
  - **Data Protection Officer (DPO)**, svolge la funzione di indirizzo e di vigilanza della protezionedeidati personali trattati da TIM e dalle Società del Gruppo, come previsto dal Regolamento UE 2016/679 (General Data Protection Regulation, GDPR) e si relaziona con l'Autorità nazionale, il Garante per protezione dei dati personali. Il compito del Data Protection Officer di sorvegliare l'osservanza della normativa sul trattamento dei dati personali è assicurato dal piano delle attività di controllo ai fini della conformità privacy eseguito dalla Direzione Compliance nell'ambito del proprio Piano annuale.
  - Il **Chief Executive Officer** che, su attribuzione del CDA e su assenso dell'autorità del Governo. ha la delega esclusiva di Amministratore sull'Organizzazione di Sicurezza, secondo quanto previsto dalla disciplina Golden Power che sancisce la stretta collaborazione con il Governo rispetto ai temi della sicurezza delle infrastrutture strategiche di comunicazione, e richiede il potenziamento dei presidi interni di sicurezza, da attuare attraverso la suddetta figura, coinvolta anche nella governance aziendale con particolare riferimento a tutti i processi decisionali afferenti ad attività strategiche e alla rete.

- **Chief Public Affairs & Security Officer (CPASO)** che, attraverso le specifiche articolazioni organizzative di Cyber Security e Sicurezza Fisica ed il Funzionario alla Sicurezza (FAS), assicura il presidio della Sicurezza delle informazioni e Cyber per il gruppo TIM, in coerenza con la disciplina del Golder Power e su attribuzione del CDA.Il Chief **Public Affairs & Security Officer** è referente unico per le tematiche di sicurezza sia Fisica sia Cyber, supervisionando le attività inerenti all'applicazione delle misure di contrasto dei rischi di Cyber Security sul perimetro di responsabilità della Società. Risponde all'Amministratore Delegato e riferisce al Comitato per il controllo e i rischi, oltre a essere il referente verso gli Organi Istituzionali. Per garantire il presidio Cyber Security, egli si avvale di processi specifici, allineati alle best practice internazionali, di prevenzione (i.e.: ICT Risk Management) e di reaction (i.e.: Monitoraggio e gestione degli incidenti di sicurezza informatica). In particolare, **l'ICT Risk Management** ha l'obiettivo di ridurre il rischio informatico, garantendo la riservatezza, l'integrità e disponibilità delle informazioni trattate, attraverso un processo di analisi delle minacce, di individuazione delle vulnerabilità e di definizione preventiva delle contromisure. Tale azione consente all'Azienda di valutare le esigenze di sicurezza dell'informazione nell'ambito degli obiettivi di business, nonché alle misure di conformità normativa in accordo con la Direzione Compliance. Il processo è disciplinato da una specifica procedura organizzativa "ICT Risk Management" e, nell'ottica del principio di *shared responsibilty*, oltre al presidio del Funzionario alla Sicurezza, prevede il coinvolgimento di tutte le funzioni che hanno responsabilità operative e presidiano i processi aziendali coinvolti.

Allo scopo di controllare l'attività di adempimento svolta dal Gruppo TIM, presso la Presidenza del Consiglio dei Ministri è istituito un apposito Comitato di Monitoraggio con il compito di verificare il rispetto delle prescrizioni imposte dal decreto e di irrogare eventuali sanzioni in caso di inottemperanza. L'azione di verifica da parte del citato Comitato di Monitoraggio ha confermato la realizzazione in TIM di elevati standard di sicurezza, con il coinvolgimento trasversale delle diverse Funzioni aziendali e con strumenti di intervento predisposti dalla Funzione Chief Public Affairs & Security Office del Gruppo TIM per garantire il quadro di indirizzo e controllo delle attività normativamente previsto a presidio dei perimetri aziendali per gli interessi di difesa e sicurezza nazionale. La collaborazione assicurata alle Istituzioni da parte del Gruppo TIM in materia di Cyber Security è costante e proficua e ne sono riprova le numerose attività svolte in seno a svariati Gruppi di Lavoro presso vari Organismi Istituzionali in cui la Security di TIM - con le Funzioni di sicurezza cyber - è presente (es. Tavoli Tecnici presso la Presidenza del Consiglio dei ministri, Ministero Interni e Ministero della Difesa).

Di seguito le figure coinvolte nel process di governance con i relativi CV:

- **Pietro Labriola, Amministratore Delegato, Direttore generale e Consigliere Delegato alla Sicurezza** https://www.gruppotim.it/it/gruppo/organizzazione/amministratore- delegato.html

- **Federico Ferro Luzzi, Presidente Comitato Controllo Rischi** 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-GiampaoloLeone.pdf

- **Agostino Nuzzolo, Direttore Legal & Tax e Data Protection Officer** https://www.gruppotim.it/content/dam/gt/sostenibilit%C3%A0/doc-varie/2022/CV-Agostino-Nuzzolo.pdf