GOVERNANCE SULLA SICUREZZA

DELL'INFORMAZIONE E SULLA CYBERSECURITY

TIM

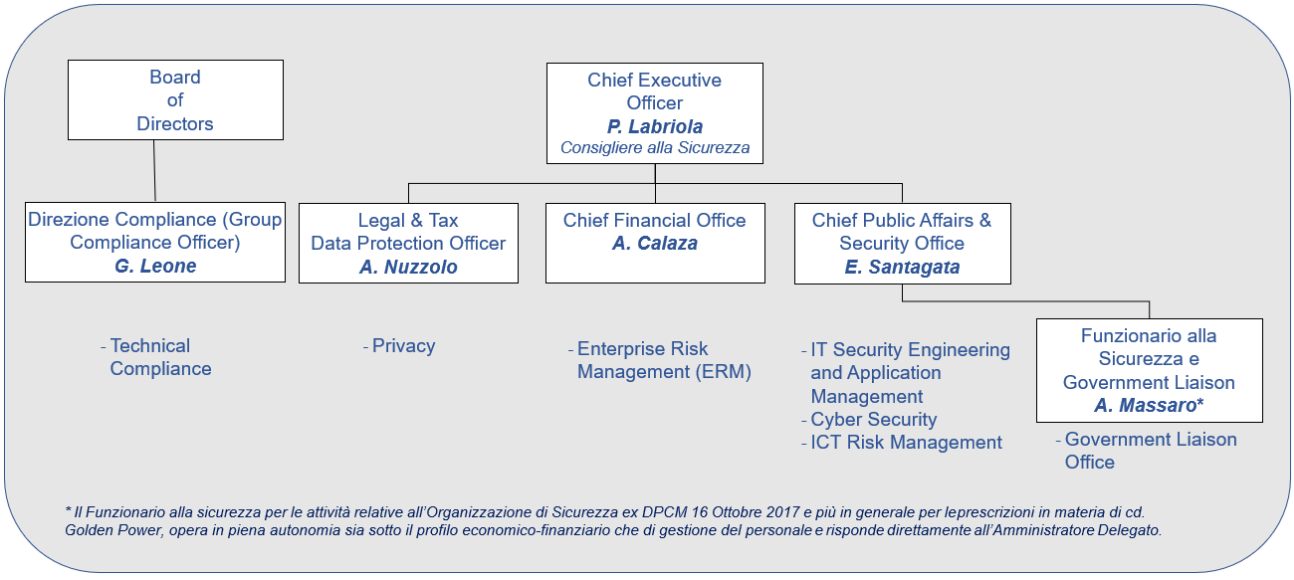
Giugno 2023

I servizi di comunicazione elettronica sono basati sulle tecnologie ICT e sono dunque essenziali al business, al governo, al presidio e al contrasto dei rischi di cybersecurity. La sicurezza delle infrastrutture, la protezione dei dati e la continuità dei servizi erogati sono prioritari per ogni operatore di telecomunicazioni, e certamente lo sono per TIM, le cui infrastrutture costituiscono storicamente l'asse portante del sistema delle comunicazioni del Paese e che si propone come un major player nazionale per i servizi di datacenter e cloud per la clientela pubblica e privata.

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 si è organizzato costituendo un comitato interno focalizzato su controlli e rischi (il Comitato per il controllo e i rischi).

Ferma la delega al Chief Executive Officer (in quanto tale, 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 mantenuto la sovra ordinazione gerarchica diretta su una funzione focalizzata anche sul presidio della conformità dei processi tecnologici e di sicurezza IT (Direzione Compliance, tramite la struttura Technical Compliance). Più in generale, a diretto riporto del CEO, il Gruppo TIM presidia i temi di Information Security e Cybersecurity Governance e gestisce i rischi associati non solo in termini diffusi e trasversali, ma avvalendosi di processi e strutture dedicati quali:

- In ambito **Public Affairs & Security Office** attraverso le strutture organizzative: **Cyber Security, ICT Risk Management, IT Security Engineering** and **Application Management** e quella relativa al Funzionario alla Sicurezza e Government Liaison
- 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)



A monte di queste scelte stanno le specificità proprie dell'Industry, autonomamente valutate da TIM, ma anche un articolato quadro normativo di emanazione nazionale e comunitario, 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 vuoi, in generale, rispetto ai servizi di comunicazione, vuoi per la difesa e la sicurezza nazionale. I c.d. decreti Golden Power, emanati nel 2017, hanno comportato l'imposizione di specifiche prescrizioni/condizioni e gravato il Gruppo TIM 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) di recente pubblicazione, 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 elettronica a banda larga con tecnologia 5G.
La robustezza delle soluzioni organizzative e gli elevati standard di sicurezza in essere sono stati riconosciuti così a livello istituzionale. Per altro verso, 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 – se possibile – la consapevolezza e l'attenzione nel perimetro cybersecurity, comportando 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 cybersecurity è così articolata:

- Il **Consiglio di Amministrazione** di TIM 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 in ambito Information Security e Cyber Security viene costantemente monitorato dalla funzione ERM l'indicatore di Sicurezza Logica ICT che misura il grado di copertura del processo di ICT Risk Management. La funzione ERM si colloca organizzativa nella Direzione Chief Financial Officer.
- Il Consiglio di Amministrazione del Gruppo TIM costituisce al proprio interno un **Comitato per il controllo e i rischi**, attualmente formato da soli amministratori indipendenti, con funzione di supporto istruttorio del plenum consiliare rispetto alle valutazioni e alle determinazioni di competenza relative al Sistema di Controllo Interno e Gestione dei Rischi. Il Comitato si riunisce secondo un proprio calendario annuale e, di regola, a precedere le riunioni del Consiglio di Amministrazione, a cui riferisce di volta in volta delle attività svolte. Nell'ambito dei rischi oggetto di considerazione dal Comitato per il controllo e i rischi rientrano con frequenza i rischi di cybersecurity e le misure a protezione della Privacy.
- 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) e la

responsabilità centrale di controllo e reporting verso il Vertice e gli Organi Societari, attribuita alla Direzione Compliance (che risponde gerarchicamente al Consiglio di Amministrazione), con una responsabilità di indirizzo ai fini della conformità delle normative di riferimento e del successivo monitoraggio delle procedure aziendali di attuazione. Il Piano annuale delle attività della Direzione Compliance è sottoposto all'approvazione del Consiglio di Amministrazione.

- Il **Data Protection Officer (DPO)**, svolge la funzione di indirizzo e di vigilanza della protezione dei dati 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.
- Ai fini di rafforzare il quadro di stretta collaborazione con il Governo rispetto ai temi della sicurezza delle infrastrutture strategiche di comunicazione, la **disciplina Golden Power** richiede – tra l'altro - il potenziamento dei presidi interni di sicurezza, da attuare attraverso la delega esclusiva a un Amministratore sull'Organizzazione di Sicurezza ed il coinvolgimento della medesima nella governance aziendale con particolare riferimento a tutti i processi decisionali afferenti ad attività strategiche e alla rete. Con l'assenso dell'Autorità di Governo, il Consiglio di Amministrazione ha attribuito questa delega al Chief Executive Officer e individuato il Funzionario alla Sicurezza, che coordina l'Organizzazione di Sicurezza, nel Responsabile della Funzione Security, che in questo modo è il referente unico per le tematiche di sicurezza sia Fisica sia Cyber. 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 Security 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 cybersecurity 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).
- Il **Funzionario alla Sicurezza** ha il compito di supervisionare e seguire le attività inerenti all'applicazione delle misure di contrasto dei rischi di cybersecurity sul perimetro di responsabilità della Società. Egli risponde all'Amministratore Delegato e riferisce d'ordinario al Comitato per il controllo e i rischi, oltre a essere il referente verso gli Organi Istituzionali. Per garantire il presidio cybersecurity, 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, il processo di ICT Risk Management ha l'obiettivo di ridurre il rischio informatico, garantendo – attraverso un processo di analisi delle minacce, individuazione delle vulnerabilità e definizione delle contromisure in via di prevenzione – la riservatezza, integrità e disponibilità delle informazioni trattate. 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. Lo sviluppo del processo viene declinato internamente al Gruppo TIM mediante opportuna procedura organizzativa “ICT Risk Management” e prevede sotto il presidio del Funzionario alla Sicurezza, nell’ottica di Shared Responsibility, il coinvolgimento di tutte le funzioni, tecnologiche e non, che hanno responsabilità operative e presidiano i processi aziendali coinvolti.

Ricapitolando, le figure coinvolte e relativi CV sono:

- **Pietro Labriola, Amministratore Delegato, Direttore generale e ConsiglieреDelegato 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 Direzione Compliance** https://www.gruppotim.it/content/dam/gt/sostenibilità/doc-varie/2022/CV-Giampaolo-Leone.pdf
- **Agostino Nuzzolo, Direttore Legal & Tax e Data Protection Officer** https://www.gruppotim.it/content/dam/gt/sostenibilità/doc-varie/2022/CV- Agostino-Nuzzolo.pdf