Linee di indirizzo del Sistema di Controllo Interno e di Gestione dei Rischi del Gruppo TIM

Consiglio di Amministrazione del 24 febbraio 2026

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

INDICE

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

1. IL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI DEL GRUPPO TIM: PRINCIPI DI RIFERIMENTO

Il Sistema di Controllo Interno e di Gestione dei Rischi (di seguito anche "SCIGR" o "Sistema") è elemento essenziale del generale assetto organizzativo di TIM S.p.A. (di seguito anche la "Società" o "TIM") e del relativo gruppo (di seguito anche "Gruppo TIM" o "Gruppo") ed è costituito dall'insieme delle strutture organizzative, delle regole e delle procedure aziendali finalizzate a garantire un effettivo ed efficace processo di identificazione, misurazione, gestione e monitoraggio dei principali rischi, con lo scopo di contribuire al successo sostenibile del Gruppo TIM, anche attraverso la definizione di adeguati flussi informativi volti a favorire il coordinamento e la circolazione delle informazioni tra i vari attori dello SCIGR. Un efficace SCIGR contribuisce a una conduzione dell'impresa coerente con gli obiettivi aziendali definiti dal Consiglio di Amministrazione, favorendo l'assunzione di decisioni consapevoli e concorre ad assicurare:

i) la salvaguardia del patrimonio aziendale;

ii) l'efficienza e l'efficacia dei processi aziendali;

iii) l'affidabilità delle informazioni fornite agli organi sociali ed al mercato;

iii) il rispetto di leggi e regolamenti, dello Statuto Sociale, e degli strumenti normativi interni.

Lo SCIGR di TIM è stato sviluppato e definito tenendo conto delle indicazioni del Codice di Corporate Governance di Borsa Italiana[1] (*"Codice di Corporate Governance"*), dei Principi di autodisciplina di TIM, delle *best practice* di riferimento e dei *framework* metodologici maggiormente riconosciuti e diffusi a livello internazionale ("*COSO - Internal Control*" e "*COSO - Enterprise Risk Management*"), emessi dal *Committee of Sponsoring Organizations of the Treadway Commission* ed aggiornati, rispettivamente, nel 2013 e nel 2017 nonché della serie storica degli effetti dell'applicazione dei Sistemi di Controllo Interno e Gestione dei Rischi precedentemente sviluppati

COSO Internal Control – Integrated Framework

Le presenti Linee di indirizzo si applicano a TIM S.p.A. e, secondo le modalità descritte nel presente documento, alle società da questa direttamente o indirettamente controllate (di seguito, in breve, anche "società controllate"), e hanno lo scopo di:

- identificare i principi e le responsabilità di governo, gestione e monitoraggio dei rischi connessi alle attività aziendali;
- definire gli elementi di indirizzo in capo ai diversi attori dello SCIGR, in modo da assicurare che i principali rischi afferenti al Gruppo risultino correttamente identificati, nonché adeguatamente misurati, gestiti e monitorati;

[1] Approvato a gennaio 2020 dal Comitato per la Corporate Governance.

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

- prevedere attività di controllo ad ogni livello operativo, in modo da assicurare il coordinamento e la proficua interazione tra i principali soggetti coinvolti nello SCIGR, anche attraverso lo scambio di flussi di informazione tra gli stessi.

Il Sistema di Controllo Interno e di Gestione dei Rischi del Gruppo TIM è un sistema integrato che coinvolge l'intera struttura organizzativa: al suo funzionamento sono chiamati a contribuire tanto gli organi sociali quanto le strutture aziendali secondo lo schema di seguito rappresentato e articolato in tre livelli di controllo, in linea con le normative e le best practice di riferimento

Governo: affidato al Consiglio di Amministrazione, responsabile di definire le linee di indirizzo dello SCIGR e verificarne l'adeguatezza. In questo ambito, l'istituzione e il mantenimento dello SCIGR sono affidati al *Chief Executive Officer* ("CEO"),, così da assicurare l'adeguatezza complessiva del Sistema e la sua concreta funzionalità, in una prospettiva di tipo *risk based*; a essi spetta dunque l'identificazione dei rischi e dei controlli di primo e secondo livello.

Primo livello di controllo: affidato alle singole unità operative, che identificano, monitorano e valutano i rischi di competenza e definiscono specifiche azioni di mitigazione per la loro gestione, assicurando il corretto svolgimento delle specifiche transazioni/operazioni. Tali attività di controllo sono demandate alla responsabilità primaria del *Management* e sono considerate parte integrante di ogni processo aziendale.

Secondo livello di controllo: affidato a specifiche funzioni aziendali diverse da quelle di linea/operative, che concorrono alla definizione delle metodologie di misurazione dei rischi, nonché alla loro individuazione, valutazione e monitoraggio/verifica. Inoltre, tali funzioni forniscono supporto al primo livello di controllo nella definizione ed implementazione delle azioni di mitigazione dei principali rischi.

Terzo livello di controllo: affidato alla Direzione *Audit*, che fornisce assurance indipendente e valuta l'adeguatezza del disegno e l'effettivo funzionamento dello SCIGR nel suo complesso, anche mediante la verifica dei controlli di linea nonché delle attività di controllo di secondo livello.

2. ARCHITETTURA DELLO SCIGR DI TIM

In linea con quanto previsto dal Framework "COSO - Internal Control", il processo di definizione e implementazione dello SCIGR di TIM è un processo continuo, volto al miglioramento dello stesso nel suo complesso, integrato nelle attività aziendali, svolto dalle persone attraverso le attività poste in essere nel perseguimento degli obiettivi aziendali e soggetto a valutazione periodica.

In particolare, lo SCIGR di TIM è strutturato coerentemente con i seguenti elementi:

1. ambiente di controllo;
2. valutazione dei rischi;
3. attività di controllo;
4. informazioni e comunicazione;
5. monitoraggio.

2.1 AMBIENTE DI CONTROLLO

L'ambiente di controllo descrive un insieme di standard, processi e strutture che forniscono la base per lo svolgimento dei controlli in tutta l'organizzazione.

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Il Consiglio di Amministrazione di TIM svolge un ruolo di indirizzo e supervisione strategica, perseguendo l'obiettivo primario della creazione di valore per gli azionisti in un orizzonte di medio-lungo periodo, tenendo altresì conto dei legittimi interessi dei restanti *stakeholders*, nella prospettiva del successo sostenibile dell'impresa.

L'ambiente interno e la cultura aziendale sono indirizzati dal Consiglio di Amministrazione della Società. L'esperienza, l'indipendenza e l'integrità etica dei Consiglieri, il loro rigore e impegno nel controllo delle attività e nella supervisione della conduzione aziendale sono fattori fondamentali dell'ambiente interno che contribuiscono in maniera determinante all'efficacia dello SCIGR.

Il Consiglio di Amministrazione e il management di TIM a tutti i livelli dell'organizzazione dimostrano, attraverso le loro direttive, azioni e comportamenti, l'importanza dell'integrità e dei valori etici a sostegno del funzionamento dello SCIGR (Tone at the Top).

Il Consiglio di Amministrazione adotta il Codice Etico e di Condotta del Gruppo, in cui sono enunciati i valori fondamentali e i comportamenti attesi nello svolgimento delle attività aziendali e nella gestione dei rapporti che ne derivano, anche con i fornitori e i business partners.

Lo SCIGR di TIM prevede processi di valutazione dell'aderenza dei comportamenti delle persone agli standard di condotta. A tal proposito, il Sistema Disciplinare adottato da TIM e descritto nel Modello 231 è finalizzato a sanzionare il mancato rispetto dei principi, delle misure e regole comportamentali indicate nel Codice Etico, nel Modello stesso nonché nelle procedure di attuazione.

L'insieme dei principi e delle regole che guidano l'esecuzione delle attività volte al perseguimento degli obiettivi aziendali, la gestione dei rischi a essi associati e le attività di controllo e di monitoraggio sono definiti nell'ambito degli strumenti normativi (in primis Policy, Procedure e Istruzioni Operative) che il Gruppo adotta e diffonde a tutta l'organizzazione, considerandoli strumenti fondamentali di *knowledge management*.

Il management definisce: (i) ruoli e responsabilità relativi alla pianificazione, esecuzione e controllo delle attività aziendali garantendo l'applicazione del principio di *segregation of duties*, nel rispetto delle linee gerarchiche definite, della diversità dei ruoli e della *mission* aziendale; (ii) flussi informativi e di reporting.

TIM si impegna ad attrarre, sviluppare e trattenere persone competenti e in linea con gli obiettivi aziendali. In particolare, la valorizzazione delle persone, il presidio e lo sviluppo delle competenze sono fondamentali per il raggiungimento, in generale, degli obiettivi aziendali e, nello specifico, delle finalità dello SCIGR. A tal fine, il Management di TIM, con il supporto delle competenti funzioni aziendali, assicura la presenza di persone con competenze adeguate a soddisfare i fabbisogni aziendali, attraverso:

- un percorso di selezione trasparente e documentato, basato su processi e metodologie definite, applicate uniformemente;
- iniziative di formazione per lo sviluppo professionale e manageriale delle persone;
- l'utilizzo di appropriati sistemi di valutazione delle persone per la rilevazione dei comportamenti lavorativi, dei risultati, delle conoscenze professionali, delle esperienze e delle potenzialità al fine di orientarne adeguatamente i percorsi di crescita e sviluppo, anche in funzione dei fabbisogni aziendali;
- sistemi di remunerazione volti a valorizzare le persone in coerenza con i livelli di responsabilità attribuiti e le professionalità acquisite. Questi possono inoltre integrare, nella componente variabile, obiettivi legati al rafforzamento del Sistema di Controllo Interno e Gestione dei Rischi con lo scopo di rafforzare la cultura e la sensibilità del Management a tali tematiche).

2.2 VALUTAZIONE DEI RISCHI

Il Gruppo TIM, ispirandosi alle linee guida dello standard ISO 31000: 2018 e ai principi del COSO - ERM Framework, adotta un Processo di Enterprise Risk Management (di seguito "ERM") finalizzato a identificare, valutare, trattare e monitorare gli eventi potenziali il cui accadimento possa influenzare il raggiungimento dei principali obiettivi aziendali definiti nel Piano Industriale. Tale processo fornisce un quadro unitario ed aggiornato dell'esposizione al rischio supportando il processo decisionale e

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

consentendo una gestione del rischio consapevole.

Il processo ERM di TIM, oltre ad essere coerente al contesto esogeno ed endogeno con cui il Gruppo si relaziona, è collegato agli obiettivi aziendali più rilevanti in termini di impatto economico-finanziario al fine del loro conseguimento. Il processo ERM del Gruppo TIM promuove, infatti, ove possibile, l'utilizzo di un approccio basato su una valutazione quantitativa del rischio, correlata al livello di impatto e alla probabilità di accadimento.

I rischi a cui è soggetto il Gruppo TIM sono valutati non solo singolarmente, ma anche in un'ottica di portafoglio e sono monitorati nel continuo al fine di rilevare tempestivamente i cambiamenti del contesto esterno e interno e i livelli di scostamento rispetto alle soglie di accettazione del rischio (c.d. *Risk Appetite*, *Risk Tolerance*), e, conseguentemente, identificare le necessarie azioni da intraprendere.

Il modello ERM viene rivisto e aggiornato periodicamente al fine di garantirne l'allineamento alle *best practice* di riferimento ed il miglioramento continuo (in termini di qualità ed efficacia) anche sulla base dell'esperienza maturata.

Inoltre, vengono assicurate a livello di Gruppo TIM le attività di gestione delle frodi e degli abusi perpetrati da terzi ai danni dell'Azienda, attraverso l'analisi dei potenziali rischi di frode/abuso, la valutazione dei presidi antifrode esistenti, la definizione delle contromisure, il monitoring, l'analisi e la detection dei fenomeni presuntivamente fraudolenti/abusivi.

2.3 ATTIVITÀ DI CONTROLLO

Le attività di controllo definite ed implementate dal Gruppo TIM sono direttamente correlate all'individuazione dei rischi aziendali (*Risk Assessment*), con l'obiettivo di prevedere misure finalizzate alla loro prevenzione, mitigazione e governo, tenendo conto della propensione e della tolleranza al rischio.

Tali attività di controllo sono integrate nei processi operativi, comprendono diversi tipi di controlli (manuali, automatici, preventive e detective), coinvolgono tutti i livelli organizzativi e includono un insieme di diverse operazioni/attività (approvazioni, autorizzazioni, verifiche, raffronti documentali, esame dei risultati, controlli sui sistemi informativi, separazione dei compiti, ecc). TIM pone particolare attenzione all'implementazione di un solido sistema di controlli sui sistemi informatici e sugli aspetti di sicurezza dei dati, delle applicazioni, degli asset e delle infrastrutture di rete.

Processi, ruoli e ambiti di responsabilità relativi alle attività di controllo sono definiti nell'ambito delle policy e procedure aziendali. In generale, la responsabilità sul funzionamento dei controlli è attribuita a tutte le risorse di TIM, in relazione alla propria attività e competenza, che intervengono prontamente qualora sia necessario intraprendere azioni correttive volte a garantire un'adeguata operatività dei controlli.

In particolare, le principali attività di controllo implementate si identificano con quelle riferite a:

a. Modello Organizzativo 231, che definisce Standard di Controllo Generali e Specifici atti a presidiare rischi di commissione dei reati previsti dal D.Lgs. 231/2001; pone l'accento sui principi di comportamento attesi ed i presidi di controllo esistenti nell'ambito dei processi aziendali sensibili alla possibile commissione di reati presupposto 231;

b. il sistema di "*whistleblowing*" che consente di segnalare, anche in forma anonima, comportamenti riferibili al personale TIM e/o a terzi in rapporti di affari con la Società, non conformi/in violazione a leggi, regolamenti e normative in genere, al Codice Etico e di Condotta ed al Modello 231, nonché al sistema di regole e procedure vigenti nel Gruppo;

c. sistema di controllo interno sul *financial reporting* (ex Legge n. 262/2005);

d. sistema di controllo interno sulla Rendicontazione di Sostenibilità (ex Decreto Legislativo n. 125/2024)

e. sistema per il controllo e la gestione dei rischi fiscali (*Tax Control Framework*);

f. Sistema di Gestione Anticorruzione (SGA) - certificato ex Standard UNI ISO 37001, al fine di

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

supportare l'organizzazione nel prevenire, rilevare e rispondere a fenomeni legati alla corruzione, nel rispetto delle leggi anticorruzione di riferimento e degli impegni volontariamente assunti e applicabili alle sue attività;

g. sistema di controllo interno in ambito *ICT* (che include anche gli "*Information Technology General Controls*"), *cybersecurity* e *Privacy* (*GDPR*).

Oltre alle attività di controllo di primo e secondo livello, sono previsti controlli di III livello svolti da parte della Direzione Audit TIM in linea con gli Standard Internazionali per la Pratica della Professione di Internal Auditing[2] econdotti con piena indipendenza organizzativa, liberi da interferenze nella definizione dell'ambito di copertura, nell'esecuzione del lavoro e nella comunicazione dei risultati.

Tali attività sono svolte secondo un piano di audit annuale top-down risk-based, approvato dal Consiglio di Amministrazione e integrato dalle richieste degli organi di controllo e del vertice aziendale (Presidente del CDA e CEO) a fronte di rischi emergenti nel corso dell'anno e tipicamente focalizzato su aree aziendali che presentano rischi o criticità potenziali o effettive.

2.4 Informazioni e Comunicazione

Informazioni e comunicazione sono elementi necessari per il corretto funzionamento dello SCIGR a supporto del raggiungimento degli obiettivi aziendali.

TIM adotta propri processi e sistemi informativi di supporto aventi l'obiettivo di individuare, gestire e comunicare in modo completo, affidabile, sicuro e tempestivo, le informazioni rilevanti ai fini dei processi decisionali interni, dei processi di controllo e dei rapporti con i propri *stakeholders*.

In particolare, i processi di comunicazione interna di TIM supportano la condivisione a tutti i livelli dell'organizzazione degli obiettivi, dei ruoli e delle responsabilità in tema di Sistema di Controllo Interno e Gestione dei Rischi.[3]

Il Gruppo TIM comunica all'esterno le informazioni rilevanti afferenti al funzionamento dello SCIGR, attraverso la pubblicazione e la diffusione di documenti/comunicazioni/relazioni (quali, Relazioni finanziarie annuali e periodiche, Principi di Autodisciplina di TIM, Relazione sul governo societario e gli assetti proprietari, comunicazioni di non financial information, ecc.) in applicazione delle normative esterne ed interne di riferimento.

2.5 Monitoraggio

Il monitoraggio è l'insieme delle attività volte a verificare che lo SCIGR, nel suo complesso e nelle sue singole fasi, sia efficacemente disegnato ed effettivamente operativo nel tempo; consiste in un'attività di supervisione continua e/o in valutazioni di carattere specifico svolte periodicamente.

Nello specifico, il Gruppo TIM prevede un insieme di valutazioni continuative (*ongoing*) e valutazioni autonome (*separate*) sul corretto funzionamento dello SCIGR.

Le valutazioni *ongoing* sono integrate e svolte all'interno delle funzioni e dei processi aziendali e vengono adeguate in funzione dei cambiamenti che intercorrono nei processi.

Attraverso le attività di monitoraggio vengono evidenziati eventuali aspetti di non adeguatezza o aree di miglioramento dello SCIGR al fine di presidiare/mitigare ulteriormente i rischi aziendali sottostanti. Tali aspetti sono riflessi in azioni di adeguamento che il Management, o le strutture preposte, definiscono e mettono in atto.

La responsabilità del monitoraggio *ongoing* dello SCIGR è del *Management* (*Prima linea di controllo*) che verifica nel tempo la corretta individuazione e l'evoluzione dei rischi nonché l'adeguatezza ed il funzionamento dei controlli posti a loro presidio.

Le valutazioni *separate* garantiscono, invece, autonomia e obiettività di giudizio in quanto sono condotte esternamente alle funzioni monitorate. Tra queste si identificano:

[2] Emanati dall'Institute of Internal Auditors (IIA)

[3] Per quanto concerne i flussi informativi tra i diversi attori dello SCIGR di TIM, si rimanda al successivo paragrafo 5 "Coordinamento e flussi informativi tra i soggetti coinvolti nello SCIGR".

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

- *Seconda linea di controllo*:
  - attività di *assurance* previste nel piano della Direzione *Compliance*;
  - attività di *audit* esterno ai fini della Certificazione UNI ISO 37001 del SGA;
  - attività di *assurance* indipendenti sul Sistema di Controllo Interno sul *Financial Reporting* ex L.262/2005 e sul Sistema di Controllo Interno sulla Rendicontazione di Sostenibilità;
  - attività di *assurance* sul *Sistema di Gestione e Controllo del Rischio Fiscale* adottato dalla Società *(Tax Control Framework);*
  - attività di *assurance* sul *Modello Privacy* di TIM.
- *Terza linea di controllo*:
  - attività di *audit* previste nel piano di Internal Audit *risk-based* o derivanti da richieste extra-piano degli organi di controllo e del vertice aziendale a fronte di rischi emergenti.

3. PRINCIPALI ATTORI DEL SISTEMA DI CONTROLLO INTERNO E DI GESTIONE DEI RISCHI DI TIM

Il Sistema di Controllo Interno e di Gestione dei Rischi del Gruppo TIM è un sistema integrato realizzato da una pluralità di organi e unità organizzative aziendali, le cui componenti risultano interdipendenti e caratterizzate da complementarità nelle finalità perseguite, nelle caratteristiche di impianto e nelle regole di funzionamento.

Di seguito viene rappresentata una vista di sintesi dei principali attori dello SCIGR rispetto al modello di Corporate Governance adottato da TIM in linea con le indicazioni del Codice di Corporate Governance e con l'architettura basata su tre livelli di controllo.

3.1 CONSIGLIO DI AMMINISTRAZIONE

Il Consiglio di Amministrazione svolge un ruolo centrale nell'ambito dello SCIGR, in considerazione della propria funzione di indirizzo e valutazione dell'adeguatezza del Sistema stesso. A tal fine, il Consiglio di Amministrazione, in particolare:

- definisce le presenti Linee di indirizzo per l'intero Gruppo, compatibilmente con l'ottemperanza alle discipline locali applicabili, affidandone l'istituzione ed il mantenimento al *Chief Executive Officer*;
- approva il Codice Etico e di Condotta del Gruppo e il Modello di organizzazione, gestione e controllo ai sensi D.lgs. 231/01;

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

- verifica l'adeguatezza, l'efficacia e il corretto funzionamento dello SCIGR, affinché i principali rischi aziendali siano correttamente identificati, gestiti e monitorati nel tempo, determinando inoltre il grado di compatibilità di tali rischi con una gestione dell'impresa coerente con gli obiettivi strategici individuati. A tal fine, valuta con cadenza semestrale l'adeguatezza e l'efficacia dello SCIGR rispetto alle caratteristiche della Società e al profilo di rischio assunto, prendendo in considerazione altresì gli esiti della valutazione effettuata dalla Direzione *Audit* anche sulla base dei contributi ricevuti dalle altre funzioni di controllo; in questo ambito definisce il livello e il tipo di rischio che la società è in grado di assumere, coerentemente con gli obiettivi strategici perseguiti nel lungo periodo (cosiddetto Risk Appetite);
- istituisce al suo interno il Comitato per il controllo e i rischi, con il supporto del quale effettua le valutazioni e assume le decisioni relative allo SCIGR, e altri comitati (Comitato per le nomine e la remunerazione, Comitato sostenibilità e Comitato parti correlate) con funzioni consultive, propositive o istruttorie, descritte nei Principi di Autodisciplina di TIM e negli appositi regolamenti;
- nomina e revoca i Responsabili delle Funzioni di Controllo di TIM *(Audit* e *Compliance*) stabilendone la remunerazione, su parere conforme del Comitato per il controllo e i rischi, sentito il Collegio Sindacale, e assicura che gli stessi siano dotati di adeguate risorse per l'espletamento delle proprie funzioni;
- approva l'Audit Charter, che definisce finalità, poteri e responsabilità della Direzione *Audit* di TIM S.p.A.;
- nomina, previo parere del Collegio Sindacale, il Dirigente Preposto alla redazione dei documenti contabili societari di TIM S.p.A. ("Dirigente Preposto"), vigilando affinché quest'ultimo disponga di adeguati poteri e mezzi per l'esercizio dei compiti a lui attribuiti dalla legge, nonché sull'effettivo rispetto delle procedure amministrative e contabili per la formazione del bilancio d'esercizio e del bilancio consolidato, così come di ogni altra comunicazione di carattere finanziario, predisposte dal medesimo Dirigente Preposto;
- ha facoltà di nominare, previo parere del Collegio Sindacale, un dirigente responsabile della rendicontazione di sostenibilità, diverso dal Dirigente Proposto al quale attribuire i poteri e le responsabilità in materia di cui all'art. 154-bis, comma 5-ter, del Decreto Legislativo n. 58/1998;
- nomina i componenti dell'Organismo di Vigilanza ex D.lgs. 231/2001, sentito il parere del Comitato per il controllo e i rischi e del Collegio Sindacale;
- approva con cadenza almeno annuale, sentito il Comitato per il controllo e i rischi, il Piano della Direzione *Compliance* e il Piano di Audit della Direzione *Audit*;
- esamina e approva la bozza di bilancio, individuale e consolidato, annuale e semestrale, e la relazione sulla gestione accompagnatoria del medesimo, redatte dal Dirigente Preposto, nonché la rendicontazione di sostenibilità redatta ai sensi del Decreto Legislativo n. 125/2024;
- valuta, sentito il Collegio Sindacale, i risultati esposti dalla società di revisione legale nella eventuale lettera di suggerimenti e nella relazione sulle questioni fondamentali emerse in sede di revisione legale;
- valuta le scelte strategiche in materia di *cybersecurity* secondo le normative di riferimento quali, ad esempio, la Network and Information Security Directive 2 (di cui alla Direttiva UE 2022/2555, "NIS 2", e al Decreto Legislativo n. 138/2024). In questo ambito approva le misure di gestione dei rischi per la sicurezza informatica, sovraintende la relativa implementazione, ricevendo specifica informativa riguardo al piano di attuazione delle misure, agli incidenti e alle attività di formazione tramite il Comitato per il controllo e i rischi e/o il Chief Executive Officer e/o la funzione Chief Security Office.

Inoltre, al Presidente del Consiglio di Amministrazione (ove non abbia incarichi esecutivi) è attribuito il ruolo di raccordo fra il Consiglio di Amministrazione e i Responsabili delle Funzioni di Controllo.

3.2 COMITATO PER IL CONTROLLO E I RISCHI

Il Comitato per il controllo e i rischi (CCR), nominato dal Consiglio di Amministrazione, svolge compiti di natura istruttoria, consultiva e propositiva essenzialmente verso il plenum consiliare (direttamente o in coordinamento con il Presidente del Consiglio di Amministrazione); ha altresì facoltà di esprimere indirizzi e raccomandazioni direttamente al *Chief Executive Officer* o al *Management*, dandone tempestiva comunicazione al Presidente del Consiglio di Amministrazione. In particolare, tra i compiti ad esso attribuiti:

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

- monitora l'osservanza delle regole di corporate governance aziendali, l'evoluzione normativa e delle best practice in materia di controlli e corporate governance, anche al fine di valutare e proporre aggiornamenti delle regole e delle prassi interne della Società e del Gruppo;
- valuta, sentiti il Dirigente Preposto alla redazione dei documenti contabili societari, il revisore legale e il Collegio Sindacale, il corretto utilizzo dei princìpi contabili e la loro omogeneità ai fini della redazione del bilancio consolidato;
- istruisce la comunicazione finanziaria e non finanziaria di periodo, in vista dell'esame da parte del plenum consiliare;
- assiste il Consiglio di Amministrazione nell'attività di vigilanza sull'adeguatezza dei poteri e mezzi a disposizione del Dirigente Preposto, nonché sul rispetto effettivo delle procedure amministrative e contabili;
- esprime pareri nei casi indicati nel precedente paragrafo 3.1 e svolge gli ulteriori compiti ad esso attribuiti dal Consiglio di Amministrazione, supportandolo nell'espletamento delle attività a quest'ultimo demandate dai Principi di Autodisciplina di TIM in materia di SCIGR;
- riceve informativa, anche tramite la funzione Chief Security Office, sull'attuazione delle misure di gestione dei rischi per la sicurezza informatica, relazionando al riguardo al Consiglio di Amministrazione;
- esprime pareri su specifici aspetti inerenti alla identificazione dei principali rischi aziendali e supporta le valutazioni e le decisioni del Consiglio relative alla gestione di rischi derivanti da fatti pregiudizievoli di cui quest'ultimo sia venuto a conoscenza;
- esamina le relazioni periodiche predisposte dalle funzioni con compiti di secondo livello di controllo aventi per oggetto l'attività di identificazione, valutazione, gestione e monitoraggio dei principali rischi aziendali;
- monitora l'autonomia, l'adeguatezza, l'efficacia e l'efficienza della Funzione di Internal Audit, anche con riferimento all'implementazione del Piano di Audit;
- può incaricare la Direzione *Audit* dello svolgimento di verifiche su specifiche aree operative;
- acquisisce gli esiti delle attività della Direzione *Audit*, analizzando i report e le relazioni periodiche contenenti informazioni sulle attività svolte, ivi inclusa la valutazione del sistema di controllo interno e gestione dei rischi;
- riferisce al Consiglio di Amministrazione, con cadenza almeno semestrale, sull'attività svolta nonché sull'adeguatezza del SCIGR;
- svolge gli ulteriori compiti a esso eventualmente attribuiti dal CdA[4].

Il Presidente del CCR è inoltre informato, contestualmente al Presidente del Consiglio di Amministrazione, al *Chief Executive Officer*, al Presidente del Collegio Sindacale e al Presidente dell'Organismo di Vigilanza[5], circa l'avvio degli interventi di audit.

Nel caso in cui il Presidente del Consiglio di Amministrazione abbia un ruolo esecutivo, al Presidente del CCR è affidato il ruolo di raccordo fra i responsabili delle funzioni di controllo e il Consiglio di Amministrazione.

Al fine di garantire un adeguato coordinamento tra i diversi organi e funzioni coinvolti nello SCIGR, alle riunioni del Comitato Controllo e Rischi partecipa il Presidente del Collegio Sindacale o altro Sindaco effettivo da lui designato; possono comunque partecipare anche gli altri Sindaci effettivi.

3.3 COLLEGIO SINDACALE

Il Collegio Sindacale svolge i compiti a esso attribuiti ai sensi di legge (e, in particolare, dall'art. 149 del TUF e dall'art. 19 del d.lgs. 39/2010) vigilando:

- sull'osservanza della legge e dello statuto sociale;

[4] Maggiori dettagli in merito ai compiti e alle modalità di funzionamento del CCR sono riportati nel Regolamento specifico pubblicato sul sito internet della Società.
[5] Con esclusivo riferimento all'ambito di TIM S.p.A.

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

- sul rispetto dei principi di corretta amministrazione;
- sull'adeguatezza della struttura organizzativa della società per gli aspetti di competenza, del sistema di controllo interno e del sistema amministrativo-contabile, nonché sull'affidabilità di quest'ultimo nel rappresentare correttamente i fatti di gestione;
- sul processo di informativa finanziaria e di sostenibilità;
- sulla revisione legale dei conti annuali e consolidati, nonché sull'indipendenza della società di revisione.

In coerenza con quanto previsto dal Codice di Corporate Governance, il Collegio Sindacale vigila sull'efficacia dello SCIGR e, a tal fine, è destinatario dei flussi informativi necessari per l'esercizio dei propri compiti. In tale ambito, il Collegio Sindacale:

- può richiedere alla Direzione *Audit* di predisporre tempestivamente relazioni su eventi di particolare rilevanza;
- riceve i report di Audit nonché le relazioni periodiche predisposti dalla Direzione *Audit,* ivi inclusa la valutazione del sistema di controllo interno e gestione dei rischi.

Inoltre, il Presidente del CS è informato, contestualmente al Presidente del Consiglio di Amministrazione, al *Chief Executive Officer*, al Presidente del CCR e al Presidente dell'Organismo di Vigilanza[6], circa l'avvio degli interventi di audit.

Il Collegio Sindacale scambia con il CCR le informazioni rilevanti per l'espletamento dei propri compiti.

Il Presidente del Collegio Sindacale, o altro Sindaco di volta in volta da questi designato, partecipa ai lavori del CCR e degli altri comitati endoconsiliari, ferma restando comunque la facoltà degli altri Sindaci di partecipare alle riunioni.

3.4 ORGANISMO DI VIGILANZA

L'Organismo di Vigilanza ex D.lgs. 231/2001 (di seguito anche "OdV"), nominato dal Consiglio di Amministrazione, svolge i seguenti compiti:

- vigila sulla complessiva adozione del Modello 231 e sulla sua diffusione all'interno dell'azienda;
- verifica nel tempo l'adeguatezza del Modello 231 promuovendone l'aggiornamento;
- verifica l'effettiva attuazione del Modello 231, anche attraverso un piano di controlli, riferendo al Consiglio di Amministrazione, al CCR e al Collegio Sindacale, con apposita relazione semestrale, in merito all'esito delle attività di vigilanza svolte nel corso del periodo, con particolare riferimento al monitoraggio dell'attuazione del Modello 231 ed alle eventuali innovazioni legislative in materia di responsabilità amministrativa degli enti. La relazione semestrale è trasmessa altresì al Presidente del CdA e all'Amministratore Delegato;
- è owner del processo di gestione delle Segnalazioni (*Whistleblowing*) riguardanti TIM S.p.A., ferme le responsabilità e le prerogative del Collegio Sindacale sulle segnalazioni allo stesso indirizzate, ivi incluse le denunce ex art 2408 Codice Civile;
- riceve i report di Audit, con riferimento all'ambito di TIM S.p.A., nonché le relazioni periodiche predisposte dalla Direzione Audit, ivi inclusa la valutazione del sistema di controllo interno e gestione dei rischi. Il Presidente dell'OdV è informato, contestualmente al Presidente del Consiglio di Amministrazione, al *Chief Executive Officer*, al Presidente del CCR e al Presidente del CS, circa l'avvio degli interventi di audit su TIM S.p.A.

L'OdV interloquisce periodicamente con il Collegio Sindacale, nel rispetto della reciproca autonomia, al fine di scambiare informazioni e documenti relativi allo svolgimento dei propri compiti e alle problematiche emerse a seguito dell'attività di vigilanza espletata.

Nell'espletamento dei propri compiti, l'OdV si coordina con la Direzione *Audit* e con la Direzione *Compliance* per gli aspetti di rispettiva competenza.

In particolare, la Direzione *Audit* supporta l'OdV tramite un'apposita Segreteria tecnica e svolge le attività

[6] Con esclusivo riferimento all'ambito di TIM S.p.A.

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

di analisi istruttoria sulle segnalazioni ricevute (*Whistleblowing*) e le attività di controllo relative al Piano di Vigilanza.

La Direzione *Compliance* supporta le attività di aggiornamento del Modello 231, di gestione dei flussi informativi ordinari e ad evento, di formazione sulle tematiche 231, nonché di monitoraggio dell'evoluzione normativa e giurisprudenziale in materia di responsabilità degli enti. In questo ambito il Responsabile della Direzione Compliance (*Group Compliance Officer)* informa l'OdV a riguardo delle iniziative adottate in materia 231 da parte dello *Steering Committee* 231 (cfr par. 3.6.1).

I ruoli e i compiti dell'Organismo di Vigilanza, nonché i flussi informativi che lo riguardano, sono dettagliati nel Modello 231, al quale si rinvia.

3.5 CHIEF EXECUTIVE OFFICER

L'Amministratore Delegato è incaricato dell'istituzione e del mantenimento del Sistema di Controllo Interno e di Gestione dei Rischi, ai sensi del Codice di Corporate Governance e dei Principi di Autodisciplina TIM.

In particolare:

- cura l'identificazione dei principali rischi aziendali, tramite il processo di Enterprise Risk Management, rispetto agli ambiti operativi coperti da delega, tenendo conto delle caratteristiche delle attività svolte dalla società e dalle sue controllate, e li sottopone periodicamente all'esame del CdA;
- dà esecuzione alle linee di indirizzo definite dal Consiglio, curando la progettazione, realizzazione e gestione del Sistema di controllo interno e Gestione Rischi e verificandone costantemente l'adeguatezza e l'efficacia nonché curandone l'adattamento alla dinamica delle condizioni operative e del panorama legislativo e regolamentare, coadiuvato dallo Steering Committee "Sistema di Controllo Interno e Gestione Rischi" (*v. par. successivo*);
- riferisce al Comitato per il controllo e i rischi in merito alle problematiche e alle criticità emerse nello svolgimento della sua attività;
- può richiedere alla Direzione *Audit* lo svolgimento di verifiche su specifiche aree operative e sul rispetto delle regole e procedure interne nell'esecuzione di operazioni aziendali dandone contestuale comunicazione al Presidente del Consiglio di Amministrazione, al Presidente del Comitato per il controllo e rischi e al Presidente del Collegio Sindacale;
- è informato, contestualmente al Presidente del Consiglio di Amministrazione, al Presidente del CCR, al Presidente del CS e al Presidente dell'Organismo di Vigilanza[7], circa l'avvio degli interventi di audit;
- riceve i report di Audit predisposti dalla Direzione Audit, anche ai fini dell'implementazione di azioni di rafforzamento del sistema di controllo interno e di gestione dei rischi.

3.5.1 *Steering Committee* "Sistema di Controllo Interno e Gestione Rischi"

Lo *Steering Committee* "Sistema di Controllo Interno e Gestione Rischi" coadiuva l'Amministratore Delegato nel dare esecuzione ed attuazione agli indirizzi stabiliti dal Consiglio di Amministrazione in merito al Sistema di Controllo Interno e di Gestione dei Rischi del Gruppo TIM.

In particolare, tale Comitato manageriale, presieduto dall'Amministratore Delegato e composto dai Responsabili della Direzione *Compliance (Group Compliance Officer),* della Funzione *Legal, Regulatory & Tax*, della Funzione *Chief Financial Office* e della Funzione *Chief Human Resources & Organization Office*, ha il compito di:

- identificare e definire le iniziative di evoluzione dello SCIGR, a sostegno dello sviluppo di una cultura orientata ai valori dell'etica, dell'integrità e del rispetto delle normative interne ed esterne;
- assicurare l'analisi integrata delle risultanze derivanti dalle attività svolte da parte delle Funzioni di controllo e di tutte le altre Funzioni che compongono il sistema, al fine di supportare ed indirizzare, ove necessario, l'implementazione delle azioni di rimedio previste, tenuto anche conto della rilevanza degli esiti.

[7] Con esclusivo riferimento all'ambito di TIM S.p.A.

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

Alle riunioni del Comitato è prevista la partecipazione in forma stabile del Responsabile della Direzione Audit.

3.6 FUNZIONI DI CONTROLLO DI PRIMO LIVELLO - *MANAGEMENT*

Il primo livello di controllo è ricoperto dal *Management* che è il primo responsabile delle attività di controllo interno e di gestione dei rischi previste a livello di Sistema. In tal senso, il *Management* ha la responsabilità di contribuire all'adeguatezza ed efficacia dello SCIGR, anche attraverso la valutazione dei rischi, l'identificazione di specifiche azioni migliorative, il corretto svolgimento delle attività nonché, attraverso la formalizzazione di procedure che regolino i processi, l'istituzione di specifiche attività di controllo, anche avvalendosi del supporto delle funzioni con compiti di secondo livello di controllo, e processi di monitoraggio idonei ad assicurare l'efficacia e l'efficienza dello SCIGR nel tempo.

Inoltre, il *Management* fornisce collaborazione alle funzioni di controllo di II e III livello ai fini dello svolgimento delle attività di *assurance*.

3.7 FUNZIONI DI CONTROLLO DI SECONDO LIVELLO

Le funzioni di controllo di secondo livello hanno compiti specifici e responsabilità di controllo su diverse aree/tipologie di rischio. Tali funzioni monitorano i rischi aziendali, propongono le linee guida con riferimento ai relativi sistemi di controllo e verificano l'adeguatezza degli stessi al fine di assicurare:

- efficienza ed efficacia delle operazioni;
- adeguato controllo dei rischi nella conduzione del business;
- affidabilità delle informazioni;
- conformità a leggi, regolamenti e procedure interne.

Le funzioni preposte a tali controlli sono autonome e distinte da quelle operative e contribuiscono al processo periodico di valutazione del SCIGR, fornendo alla Direzione *Audit* informazioni rilevanti sullo SCIGR e/o giudizi di adeguatezza dello stesso con specifico riferimento agli ambiti di propria competenza.

3.7.1 Direzione *Compliance*

Un ruolo di specifica rilevanza nell'ambito dello SCIGR del Gruppo TIM è ricoperto dalla Direzione *Compliance*, con riferimento alla prevenzione del rischio di non conformità dell'attività aziendale alle normative di riferimento.

La Direzione *Compliance*, che dipende gerarchicamente dal Consiglio di Amministrazione, in materia di gestione dei rischi ha la missione di presidiare i principali fattori di rischio di non conformità alle vigenti normative esterne (norme cogenti) e interne (procedure aziendali) e di supportare il Vertice aziendale e il *management* nella definizione delle azioni a mitigazione di tali fattori di rischio.

In particolare, ai fini della *compliance* alle normative sul *financial reporting*, la Direzione Compliance, ferma restando la responsabilità del processo attribuita al Dirigente Preposto, si occupa della definizione e dell'aggiornamento della metodologia adottata e del monitoraggio del processo end-to-end, sovraintende al disegno dei controlli ed è responsabile per le attività di *assurance* (test indipendenti, verifica del superamento delle carenze di controllo) a supporto del processo d'attestazione. L'attività di *assurance* viene assicurata altresì in materia di rendicontazione di sostenibilità. In tale ambito Direzione Compliance fornisce supporto al Dirigente responsabile della rendicontazione di sostenibilità ai fini del processo di attestazione con riferimento agli aspetti metodologici e di disegno dei controlli, oltre ad assicurare il monitoraggio dello stesso e l'effettuazione di test indipendenti.

Inoltre, la Direzione *Compliance* supporta gli Organismi di Vigilanza ex Decreto Legislativo n. 231/2001 delle società controllate nazionali nell'espletamento dei compiti a loro attribuiti.

Infine, alla Direzione *Compliance* è attribuito il ruolo di funzione di conformità per la prevenzione della corruzione, responsabile dell'attuazione e del monitoraggio del Sistema di Gestione Anticorruzione all'interno dell'organizzazione aziendale e, più in generale, della sua conformità ai requisiti della norma UNI ISO 37001.

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

3.7.2 Dirigente Preposto alla redazione dei documenti contabili societari

Il Dirigente Preposto alla redazione dei documenti contabili della Società, nominato dal Consiglio di Amministrazione previo parere del Collegio Sindacale, è uno dei principali soggetti coinvolti nel funzionamento del Sistema di controllo interno e gestione dei rischi, in quanto responsabile:

- della definizione delle procedure amministrative e contabili necessarie per la formazione dei documenti contabili societari e di ogni altra comunicazione di carattere finanziario nonché della loro adeguatezza ed effettiva applicazione;
- della corrispondenza dei documenti contabili societari alle risultanze dei libri e delle scritture contabili e della loro idoneità a fornire una rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria della Società e del Gruppo;
- della completezza dei contenuti e in generale del rispetto della disciplina applicabile alla documentazione di bilancio;
- della redazione della bozza di bilancio, individuale e consolidato, annuale e semestrale, e della relazione sulla gestione accompagnatoria del medesimo e, in genere, della documentazione contabile da sottoporre all'esame e all'approvazione del Consiglio di Amministrazione.

Al riguardo viene emessa, congiuntamente all'Amministratore Delegato, apposita attestazione allegata al bilancio d'esercizio di TIM ed al bilancio consolidato annuale e al bilancio consolidato semestrale abbreviato.

Il Dirigente Preposto riferisce al Consiglio di Amministrazione, al Comitato per il controllo e i rischi e - per quanto di competenza - al Collegio Sindacale, in relazione alle funzioni e alle responsabilità proprie della carica.

3.7.3 Dirigente responsabile della rendicontazione di sostenibilità

Il Consiglio di Amministrazione, esercitando la facoltà prevista dallo Statuto e con il parere favorevole del Collegio Sindacale, ha designato la responsabile della Funzione *Corporate Communication & Sustainability* quale dirigente dotata di specifiche competenze in materia di rendicontazione di sostenibilità chiamata a rilasciare l'attestazione di cui all'art. 154-bis, comma 5-ter, del Decreto Legislativo 58/1998 in merito alla conformità di detta rendicontazione agli standard applicati ai sensi della regolamentazione dell'Unione Europea sul tema.

3.7.4 Pianificazione e controllo

Il Chief Financial Officer ("CFO"), oltre a ricoprire il ruolo di Dirigente Preposto, garantisce, anche tramite la struttura organizzativa dedicata, l'esecuzione di attività di controllo di secondo livello relative al monitoraggio economico- finanziario e patrimoniale della società e del Gruppo TIM.

In particolare, il CFO svolge i seguenti principali compiti:

- definisce policy, linee guida, procedure e strumenti di supporto al processo di pianificazione e controllo nonché alle attività di monitoraggio economico-finanziario e patrimoniale;
- assicura le attività di pianificazione e di controllo economico-finanziario e patrimoniale, identificando eventuali scostamenti significativi e suggerendo possibili azioni correttive per il raggiungimento degli obiettivi definiti nonché monitora i rischi economici, finanziari e patrimoniali;
- predispone una reportistica periodica verso il vertice aziendale, nonché verso il CCR, il Collegio Sindacale e il CdA di TIM sulla performance economica, finanziaria, patrimoniale e gestionale di TIM e del Gruppo, per successiva comunicazione al mercato.

3.7.5 Funzione Enterprise Risk Management

La Funzione *Enterprise Risk Management*, a riporto del CFO di TIM, svolge un ruolo di divulgazione e adozione della metodologia ERM all'interno del Gruppo al fine di identificare, valutare, trattare e monitorare i rischi impattanti il business e supporta i *Risk Owner* (soggetti responsabili della gestione del rischio) nella definizione ed implementazione delle azioni di mitigazione. In particolare:

- valuta il profilo di rischio complessivo della Società e collabora alla definizione della natura e del livello di rischio compatibile con gli obiettivi strategici della Società e alla sua attuazione (Risk Appetite);

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

- coordina il processo di identificazione, valutazione, trattamento e monitoraggio dei rischi di TIM;
- relaziona periodicamente in merito ai principali rischi di TIM e ai relativi piani di trattamento al CCR e all'Amministratore Delegato, nonché, ove richiesto, agli altri organi di controllo e vigilanza;
- promuove la diffusione della cultura di gestione del rischio a tutti i livelli aziendali, volta a contribuite allo sviluppo e alla condivisione di principi, comportamenti e attitudini secondo un approccio risk-based;
- supporta l'integrazione del processo di ERM nei principali processi aziendali (es. Internal Audit, pianificazione strategica etc.) e partecipa all'identificazione e alla valutazione dei rischi legati alle operazioni di investimento;
- fornisce supporto tecnico-metodologico allo *Steering Committee ERM*.

3.7.6 *Steering Committee ERM*

Lo *Steering Committee ERM* ha lo scopo di garantire il governo del processo di gestione dei rischi di Gruppo, coordinando il piano delle azioni preventive finalizzate ad assicurare la continuità operativa del Business e monitorando l'efficacia delle contromisure adottate. Lo *Steering Committee ERM* è presieduto dal Responsabile della Funzione *Chief Financial Office* ed è composto altresì dai Responsabili delle Funzioni *Legal, Regulatory & Tax*, *Chief Human Resources and Organization Office*, Direzione *Compliance*, *Chief Consumer, Small & Medium and Mobile Wholesale Market Office, Chief Technology Office, Chief Enterprise and Innovative Solutions Office* ed *Enterprise Risk Management*. Il Responsabile della Funzione *Chief Financial Office*, in qualità di Presidente dello *Steering Committee ERM*, assicura flussi informativi verso il Vertice del Gruppo, la Direzione *Audit*, il Comitato per il controllo e i rischi, il Collegio Sindacale e verso lo *Steering Committee "Sistema di Controllo Interno e Gestione dei Rischi*".

3.7.7 Data Protection Officer

Il *Data Protection Officer* (DPO) di TIM viene nominato con delibera del Consiglio di Amministrazione e ha il compito di supportare il management nello sviluppo e nell'implementazione di policy, procedure, controlli e tutele con riferimento alle tematiche relative alla privacy. In particolare, svolge i seguenti principali compiti:

- assicura il monitoraggio delle evoluzioni normative in ambito privacy informando il titolare ed i responsabili del trattamento (rispettivamente "Titolare" e "Responsabili") in merito alle stesse, verificando inoltre la conformità delle procedure e della documentazione aziendale alla normativa;
- definisce le linee guida in materia di privacy per tutte le società del Gruppo*;*
- fornisce, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e verifica i relativi adempimenti;
- garantisce la corretta informativa e applicazione delle normative in TIM, in raccordo con le competenti Funzioni aziendali;
- assicura il presidio dei rapporti con il Garante Privacy;
- funge da punto di contatto aziendale per gli interessati, in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;
- riferisce periodicamente al vertice e agli organi aziendali, se necessario, sui principali aspetti relativi al trattamento dei dati personali nonché, di tutti gli eventi rilevanti per la Società in ambito privacy (es. ispezioni del Garante Privacy, eventi di Data Breach, ecc.).

3.7.8 Tax Office

TIM ha aderito al regime convenzionale dell'Adempimento Collaborativo disciplinato dagli articoli 3 e seguenti del Decreto Legislativo 5 agosto 2015, n. 128. Conseguentemente, TIM ha adottato e attuato un Modello di Governance Fiscale, di cui è parte il Sistema di Controllo Interno e Gestione dei Rischi Fiscali (SCIGRTax), funzionale ad un efficace ed efficiente sistema di controllo del rischio fiscale.

La Funzione *Tax Office* ha un focus primario sulla regolamentazione aziendale delle tematiche fiscali, sull'identificazione, sulla valutazione, sulla gestione e sul monitoraggio del rischio fiscale.

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

In particolare, la Funzione *Tax Office* (nella persona del *Tax Officer* o dei suoi riporti funzionali):

- è informata delle decisioni strategiche e partecipa al processo di pianificazione operativa e finanziaria;
- è destinataria dei flussi informativi che riceve dalle Funzioni Owner della pianificazione e implementazione di:
  - ✓ operazioni di M&A (es.: acquisizioni, fusioni, scissioni, ecc.);
  - ✓ cambiamenti nella struttura organizzativa;
  - ✓ nuovi processi significativi con implicazioni in termini di conformità fiscale;
  - ✓ accordi intercompany, ancorché stipulati tra soggetti residenti;
  - ✓ accordi economici con diverse controparti (clienti, fornitori, dipendenti, altri soggetti);
- è costantemente informata delle risultanze delle attività di verifica dei vari organismi di controllo, interno ed esterno, di TIM e delle Società del Gruppo;
- riceve i verbali del Consiglio di Amministrazione con cadenza trimestrale.

Inoltre, il *Tax Officer* supporta il Responsabile della Funzione *Legal, Regulatory & Tax* nel garantire il flusso informativo verso il Comitato per il controllo e i rischi e verso il Consiglio di Amministrazione, con riferimento alle tematiche di rilevanza fiscale e ai rischi fiscali (tra cui evento e/o di processo) che potrebbero derivare.

3.7.9 Chief Security Office

La funzione Chief Security Office, a diretto riporto del Chief Executive Officer, assicura, attraverso la struttura organizzativa Cyber Security la sicurezza logica e la tutela delle risorse informatiche e infrastrutturali, degli asset ICT, nonché delle informazioni.

La funzione Cyber Security opera attraverso 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, in accordo con la Direzione Compliance e con il coinvolgimento di tutte le funzioni che hanno responsabilità operative e presidiano i processi aziendali coinvolti.

Inoltre, Chief Security Office garantisce, con riferimento alle normative applicabili in materia di sicurezza cibernetica, il monitoraggio delle azioni e la gestione dei flussi informativi, sia interni che verso gli Organismi. In tale contesto sono individuate le seguenti figure:

- il Funzionario alla Sicurezza che, nell'ambito della disciplina del Golder Power e su attribuzione del Consiglio di Amministrazione, coordina l'Organizzazione della sicurezza ed è referente unico per le tematiche di sicurezza fisica e cyber, supervisionando le attività inerenti all'applicazione delle misure di contrasto dei rischi di cyber security sul perimetro di responsabilità della Società; risponde al Chief Executive Officer e riferisce al Comitato per il controllo e i rischi, oltre a essere il referente verso gli Organi Istituzionali;
- il Punto di contatto NIS2 per TIM S.p.A.[8] che, in base ad apposta delega del Chief Executive Officer cura l'attuazione della normativa NIS2, riferisce direttamente al vertice gerarchico e agli organi di amministrazione per le tematiche di competenza ed interloquisce con l'Agenzia per la Cybersicurezza Nazionale ("ACN") per conto della Società;
- il Referente CSIRT NIS2, avente responsabilità delle comunicazioni e delle notifiche degli incidenti di sicurezza verso lo CSIRT Italia (*i.e.* il *Computer Security Incident Response Team* dell'ACN).

[8] Per le Società del Gruppo in perimetro NIS2 sono individuati specifici Punti di contatto.

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

3.7.10 Altri presidi di controllo di secondo livello

TIM ha istituito altri presidi di controllo di secondo livello, che gestiscono e monitorano specifici rischi aziendali connessi all'operatività del Gruppo (quali, ad esempio, rischi in materia di salute e sicurezza sui luoghi di lavoro ex Decreto Legislativo n. 81/2008, rischi antitrust, rischi di frode, etc.), definendo le linee guida sui relativi sistemi di controllo e verificando l'adeguatezza degli stessi attraverso attività di monitoraggio al fine di assicurare, tra l'altro, un adeguato controllo dei rischi, affidabilità delle informazioni, conformità a leggi, regolamenti e procedure interne.

3.8 FUNZIONE DI CONTROLLO DI TERZO LIVELLO – DIREZIONE *AUDIT*

La Direzione Audit di TIM, in qualità di funzione di controllo di terzo livello, svolge attività indipendente di assurance e advisory finalizzata al miglioramento dell'efficacia e dell'efficienza dello SCIGR nel suo complesso.

Il Responsabile della Direzione Audit dipende gerarchicamente dal Consiglio di Amministrazione, non è responsabile di alcuna area operativa ed è incaricato di verificare che il Sistema di Controllo Interno e di Gestione dei Rischi sia funzionante, adeguato e coerente con le linee di indirizzo definite dal Consiglio di Amministrazione.

La Direzione Audit ha accesso diretto a tutte le informazioni utili per lo svolgimento dell'incarico e opera sulla base di un mandato ("Audit Charter"), approvato dal CdA di TIM, che ne definisce il ruolo e le responsabilità, in coerenza con i principi di corporate governance del Gruppo TIM e con gli standard professionali internazionali dell'Internal Audit.

In particolare, la Direzione Audit*:*

- verifica, sia in via continuativa, sia in relazione a specifiche necessità e nel rispetto degli standard di *audit* internazionali, l'operatività e l'idoneità del SCIGR, attraverso un Piano di *audit* definito sulla base di un processo strutturato di analisi e prioritizzazione dei principali rischi. Con cadenza annuale tale Piano è sottoposto all'approvazione del Consiglio di Amministrazione, previa presentazione e discussione con il Comitato per il controllo e i rischi, sentito il Presidente, l'Amministratore Delegato e il Collegio Sindacale;

- valuta gli eventuali aggiornamenti al Piano di Audit per rischi emergenti e considera - per l'esecuzione di interventi "extra piano" - gli input ricevuti dagli organi e dal vertice aziendale, le segnalazioni pervenute ovvero gli eventi significativi o altri input intercettati in corso d'anno, riferendo le variazioni significative del Piano ai soggetti di cui al precedente capoverso;

- verifica, nell'ambito del Piano di audit, l'affidabilità dei sistemi informativi, inclusi i sistemi di rilevazione contabile;

- predispone, a seguito di ogni intervento di audit, report contenenti le risultanze dell'attività svolta e ne cura la trasmissione al Consiglio di Amministrazione, all'Amministratore Delegato, al Comitato per il controllo e i rischi, al Collegio Sindacale e, relativamente alle sole tematiche in perimetro TIM, anche all'Organismo di Vigilanza 231;

- predispone relazioni periodiche contenenti informazioni sulla propria attività, sulle modalità con cui viene condotta la gestione dei rischi, nonché sul rispetto dei piani definiti per il loro contenimento, riferendo al Comitato per il controllo e i rischi, al Collegio Sindacale e, relativamente alle sole tematiche in perimetro TIM, anche all'Organismo di Vigilanza 231;

- monitora nel corso dell'anno l'implementazione delle azioni correttive relative alle carenze riscontrate nell'ambito delle attività di audit e, nei casi di maggiore criticità, svolge attività di follow-up, al fine di verificare l'evoluzione e il rafforzamento del SCIGR;

- fornisce su base semestrale al Comitato per il controllo e i rischi e al Collegio Sindacale una valutazione sulla complessiva adeguatezza ed operatività del Sistema di Controllo Interno e di Gestione dei Rischi di TIM anche sulla base delle informazioni ricevute dagli altri assurance provider aziendali (cfr. successivo par. 4).

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

La Direzione Audit effettua la propria attività anche con riferimento alle società controllate prive di corrispondenti strutture di Audit, agendo nel loro interesse e riferendo ai rispettivi organi. Con la Funzione Audit di TIM Brasil si interfaccia, in ottica di coordinamento, omogeneizzazione ed indirizzo metodologici, compatibilmente con il rispetto delle discipline applicabili e delle responsabilità proprie di detta struttura.

Inoltre, la Direzione Audit supporta gli Organismi di Vigilanza di TIM e delle società controllate nel processo di gestione delle segnalazioni (cd. "Whistleblowing") e supporta l'Organismo di Vigilanza 231 di TIM tramite un'apposita segreteria tecnica (cfr. par. 3.4).

Il Responsabile della Funzione di Internal Audit di norma partecipa alle riunioni del CCR, del CS e dello Steering Committee "Sistema di Controllo Interno e Gestione Rischi".

3.9 STEERING COMMITTEE 231

La Società ha costituito un comitato manageriale, denominato *Steering Committee 231*, composto dal *Group Compliance Officer*, dal Responsabile della Funzione *Chief Human Resources & Organization Office* e dal Responsabile della Funzione *Legal, Regulatory & Tax*, e al quale partecipa in forma stabile il Responsabile della Direzione *Audit*.

Lo *Steering Committee 231* ha lo scopo di individuare le aree di miglioramento/integrazioni al Modello Organizzativo 231 e di coordinare la realizzazione dei relativi piani attuativi. Con riferimento al Sistema di Gestione Anticorruzione, il Comitato assume altresì la responsabilità generale sul funzionamento del SGA, assicurando la definizione delle iniziative per l'efficace adozione del SGA da parte delle Funzioni aziendali interessate.

Il comitato si riunisce su base periodica e, per il tramite del *Group Compliance Officer*, svolge altresì attività propositiva ed informativa nei confronti dell'Amministratore Delegato nonché del Consiglio di Amministrazione, attraverso il Comitato per il controllo e i rischi.

4. IL PROCESSO DI VALUTAZIONE DEL SISTEMA DI CONTROLLO INTERNO E GESTIONE DEI RISCHI

In conformità ai requisiti del Codice di Corporate Governance, TIM ha definito il processo di valutazione complessiva del Sistema di Controllo Interno e di Gestione dei Rischi, governato dal Comitato per il controllo e rischi che fornisce supporto istruttorio alle valutazioni e decisioni del CdA relative allo SCIGR.

Il CdA esprime la valutazione complessiva sulla base dei riscontri cui perviene a seguito delle attività svolte nel periodo, nonché delle informazioni rilevanti per lo SCIGR fornite dalle strutture interessate (Assurance Provider). Il processo è svolto con periodicità semestrale. In particolare:

- nel periodo luglio-agosto, il CCR, sulla base della proposta di Relazione presentata dalla Direzione *Audit*, presenta al Consiglio di Amministrazione la proposta di valutazione, contenente un'analisi dello SCIGR e una «Interim» Overall Opinion basate sui flussi informativi (v. allegato 1) rilevanti disponibili con riferimento al primo semestre dell'anno;

- nel periodo febbraio-marzo, il CCR, sulla base della proposta di Relazione presentata dalla Direzione *Audit*, presenta al Consiglio di Amministrazione la propria valutazione, contenente un'analisi di dettaglio di tutte le componenti dello SCIGR e una Overall Opinion, basate sul set completo di flussi informativi e relazioni annuali (v. allegato 1).

4.1 ATTORI COINVOLTI NEL PROCESSO DI VALUTAZIONE

- Il **Consiglio di Amministrazione** approva la "Relazione ai fini della valutazione di adeguatezza sull'attività svolta e sull'adeguatezza del SCIGR" predisposta semestralmente dal CCR.

- Il **Comitato per il controllo e i rischi** supporta il CdA nelle attività istruttorie relative al processo di valutazione dello SCIGR del Gruppo ed elabora una proposta di valutazione complessiva sull'idoneità dello stesso all'interno della "Relazione ai fini della valutazione di adeguatezza sull'attività svolta e sull'adeguatezza dello SCIGR" (avvalendosi del supporto operativo della Direzione *Audit*).

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

- Il *Chief Executive Officer*, nell'ambito delle sue attribuzioni in merito alla progettazione, realizzazione e gestione dello SCIGR e di verifica costante sulla sua adeguatezza ed efficacia, fornisce riscontro al CCR in merito al Sistema di Controllo Interno e Gestione dei Rischi di TIM.

- La Direzione *Audit* ricopre il ruolo di supporto operativo al Comitato per il controllo e i rischi e di conseguenza al CdA, ai fini della valutazione complessiva dello SCIGR, fornendo i risultati delle proprie attività nonché ulteriori informazioni utili ai fini della valutazione dello SCIGR raccolte dagli altri Assurance Provider di TIM, per gli ambiti di rispettiva competenza.

- Gli Assurance Provider e altre strutture aziendali con specifici compiti sul Sistema di Controllo Interno e Gestione dei Rischi sono coinvolti nel processo di valutazione, fornendo informazioni sulle attività svolte e su tematiche rilevanti in ambito SCIGR ed esprimendo, ove richiesto e per quanto di competenza, una valutazione in merito alla relativa adeguatezza. A titolo esemplificativo, si tratta di: Dirigente Preposto, Dirigente responsabile della rendicontazione di sostenibilità, Group Compliance Officer, Organismo di Vigilanza, Tax Office, Data Protection Officer, HSE, Enterprise Risk Management, etc.

4.2 ATTIVITÀ ISTRUTTORIA E RELAZIONE DELLA DIREZIONE AUDIT

La Direzione Audit avvia con cadenza semestrale, in coerenza con le scadenze del calendario societario in merito all'approvazione delle relazioni finanziarie (semestrali e annuali), il processo di valutazione dello SCIGR.

A tal fine:

- riceve dagli assurance provider o da altre funzioni competenti in ambito SCIGR le relazioni contenenti la sintesi delle attività svolte nel periodo e/o le principali informazioni e valutazioni di competenza rilevanti per la valutazione di adeguatezza dello SCIGR di TIM (v. Allegato 1);
- consolida e valuta in un'ottica integrata i contributi ricevuti e le risultanze delle attività di auditing svolte nel corso dell'anno;
- predispone una Relazione riepilogativa dei principali elementi rilevanti ai fini del Sistema di Controllo Interno e di Gestione dei Rischi di TIM, esprimendo una propria valutazione in merito all'adeguatezza dello SCIGR;
- trasmette la Relazione al CCR, al CS, all'OdV, al CEO, al Dirigente Preposto e al CdA.

Il Comitato per il controllo e i rischi:

- viste ed esaminate le informazioni pervenute da parte degli Assurance Provider,
- vista la Relazione ricevuta dalla Direzione Audit,
- sentito il *Chief Executive Officer*,

conclude l'attività istruttoria, riportandone gli esiti al Consiglio di Amministrazione, affinché quest'ultimo possa esprimere la propria valutazione complessiva sull'adeguatezza ed efficacia del Sistema di Controllo Interno e di Gestione dei Rischi di TIM nel periodo di riferimento.

5. COORDINAMENTO E FLUSSI INFORMATIVI TRA I SOGGETTI COINVOLTI NELLO SCIGR

Oltre alle modalità di interazione già descritte nei precedenti paragrafi, il quadro normativo interno di TIM prevede flussi informativi tra i diversi attori dello SCIGR, ovvero:

- dal Management di linea (primo livello di controllo) verso le funzioni di secondo e terzo livello di controllo;
- tra le funzioni di controllo di secondo e terzo livello;

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

- da parte delle funzioni di primo, secondo e terzo livello di controllo verso gli Organi di Amministrazione e Controllo;
- tra Organi di Amministrazione e Controllo.

Si prevedono due principali momenti di coordinamento e interazione tra le funzioni di controllo anche attraverso l'adozione dei comitati manageriali in precedenza descritti:

1. *coordinamento in fase di programmazione delle attività annuali*: le funzioni aziendali di controllo svolgono degli incontri preliminari di coordinamento in fase di programmazione delle attività per garantire un adeguato presidio dei principali rischi aziendali, consentendo, ove possibile, di operare in modo sinergico, e di individuare e gestire efficacemente le aree di sovrapposizione, evitando ridondanze e diseconomie;
2. *aggiornamenti periodici sulle valutazioni/misurazioni dei rischi e dell'adeguatezza dei controlli*: le funzioni aziendali di controllo prevedono specifici momenti di coordinamento per lo scambio di informazioni relative alle risultanze delle proprie attività e alle valutazioni effettuate sul funzionamento dello SCIGR, nonché delle relative azioni di miglioramento previste/adottate. A tal fine, per il rilascio del giudizio di idoneità da parte del CdA, sono stati definiti appositi flussi informativi periodici, come descritto nel paragrafo precedente del presente documento (v. anche Allegato 1).

6. MODALITÀ DI ATTUAZIONE NELLE SOCIETÀ CONTROLLATE

Al fine di garantire l'adeguato funzionamento dello SCIGR, coerentemente con l'attività di direzione e coordinamento svolta da TIM, gli organi amministrativi delle società controllate assicurano l'adeguamento tempestivo del Sistema di Controllo Interno e di Gestione dei Rischi alle presenti linee di indirizzo, tenuto conto della dimensione, della complessità delle attività svolte, del profilo di rischio specifico della società interessata e del relativo contesto regolamentare di riferimento.

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

ALLEGATO 1: FLUSSI PREVISTI A SUPPORTO DELLA VALUTAZIONE SCIGR

Di seguito si riporta lo schema di sintesi dei principali soggetti aziendali (assurance provider o altre funzioni) che producono, con cadenza periodica o ad hoc, relazioni/informative contenenti la sintesi delle attività di assurance svolte nel periodo e/o le principali informazioni e valutazioni di competenza rilevanti, a supporto della valutazione di adeguatezza dello SCIGR di TIM predisposta dalla Direzione Audit.

LEGENDA: ●● Flussi PERIODICI ○ Flussi "AD HOC", solo in presenza di elementi di rilievo

MITTENTE	FLUSSI INFORMATIVI	FLUSSI PERIODICI	
		Semestrale	Annuale
Affari Societari	*Informativa su eventuali cambiamenti rilevanti in materia di Corporate Governance (es. modifiche ai Regolamenti degli Organi di Controllo)*	○	○
Organismo di Vigilanza 231	*Relazione sulle attività svolte in ambito 231 e ambito Whistleblowing*	●	●
Direzione Compliance	*Relazione della Direzione Compliance (comprensiva di valutazione SCIGR sulle parti di competenza) su attività svolte in particolare in ambito D.Lgs. 231/01, Privacy, L. 262/05 e informativa finanziaria, rendicontazione di sostenibilità, ambito Anticorruzione – ISO 37001, HSE, sistemi informativi*	●	●
Data Protection Officer	*Relazione delle attività svolte (es. attività di verifica, DPIA attivate, eventuali data breach, gestione di particolari richieste degli interessati e dell'Autorità di controllo, etc.)*		●
	Eventuale informativa su eventi connessi al modello Privacy che possano risultare rilevanti ai fini della valutazione SCIGR	○	
Dirigente Preposto alla redazione dei documenti contabili societari	*Attestazione del bilancio d'esercizio e consolidato ai sensi dell'art. 81-ter del regolamento consob n. 11971 del 14 maggio 1999 e successive modifiche ed integrazioni*	●	●
Dirigente Preposto alla Rendicontazione di Sostenibilità	*Attestazione della rendicontazione di sostenibilità ai sensi dell'art. 81 - ter del Regolamento Consob n.11971 del 14 maggio 1999 e successive modifiche ed integrazioni*		●
Revisore Esterno	*Relazione sul Bilancio rilasciata dal Revisore Legale dei Conti*	●	●
Legal, *Regulatory* & Tax	*Relazione sullo stato dell'arte dello SCIGR del Rischio Fiscale di TIM e dei risultati delle attività svolte, comprensiva di una valutazione dello SCIGR Fiscale*		●
	Relazione antitrust		●
	Eventuale informativa su eventi rilevanti che impattano lo SCIGR o evoluzioni organizzative e normative interne che possano risultare rilevanti ai fini della valutazione SCIGR	○	
HSE	*Informativa sulle principali attività svolte nell'anno, eventuali novità normative rilevanti, andamento degli indici infortunistici, lo stato di implementazione di eventuali action plan definiti ed eventuali eventi critici rilevanti*	○	○
HR	• *Informativa relativa ai principali interventi organizzativi (a livello di Direzioni) intervenuti nell'anno, con indicazione sintetica dei razionali / finalità dei cambiamenti*		●

Gruppo TIM - Uso Interno - Tutti i diritti riservati.

MITTENTE	FLUSSI INFORMATIVI	FLUSSI PERIODICI	
		Semestrale	Annuale
	• *Informativa relativa ai principali interventi sul quadro normativo e procedurale (Policy, Procedure, Linee Guida, Modelli) effettuati nell'anno, che hanno inciso in maniera significativa sullo SCIGR di TIM e delle società strategiche*		
IT	*Informativa sulle principali attività svolte in tema di Sistemi Informativi, ritenute rilevanti ai fini del Sistema di Controllo Interno e Gestione Rischi (es. Cyber, Digital Transformation, rafforzamento di controlli automatici a supporto dei processi, etc.,)*	●	●
Enterprise Risk Management	• *Enteprise Risk Assessment report relativo al Piano Industriale* • *Report al monitoraggio di Appetite/Tolerance* • *altri report di analisi dei rischi (es. su progetti strategici di investimento)*	●	●
Security	*Informativa relativa ai principali eventi / temi rilevanti in ambito di Cyber Security, ICT Risk management, Business Continuity, Fraud Management e Sicurezza fisica*	●	●
Funzione Audit TIM SA (Brasile)	*Attestazione della valutazione SCIGR di TIM BRASIL*	●	●
Direzione Audit	• *Consuntivo sulle attività di controllo svolte (es. esiti attività di audit, principali rilievi, follow up, monitoraggio), anche con riferimento al Piano di Vigilanza 231* • *Consuntivo sulla gestione delle segnalazioni (es. numero segnalazioni ricevute; status gestione; principali esiti delle istruttorie ed action plan emersi, etc.)*	●	●

Gruppo TIM - Uso Interno - Tutti i diritti riservati.