esprinet®

Linee di indirizzo per il Sistema di Controllo Interno e di Gestione dei Rischi

Approvazione:	Consiglio di Amministrazione del 24/09/2009
Ultima Revisione:	Consiglio di Amministrazione del 22/01/2026

Linee di indirizzo per il Sistema di Controllo Interno e di Gestione dei Rischi

1. PREMESSA

Il Sistema di Controllo Interno e di Gestione dei Rischi (nel seguito "SCIGR") costituisce un elemento essenziale del sistema di governo societario di Esprinet S.p.A. (la "Società") e delle sue controllate e/o consociate (tutte insieme il "Gruppo").
Esso è definito come l'insieme di regole, comportamenti, politiche, procedure e strutture organizzative volte a consentire l'identificazione, la misurazione, la gestione ed il monitoraggio dei principali rischi gestionali contribuendo ad assicurare la salvaguardia del patrimonio sociale, l'efficienza e l'efficacia dei processi aziendali, l'affidabilità dell'informazione finanziaria e della rendicontazione di sostenibilità, il rispetto di leggi e regolamenti nonché dello statuto sociale e delle procedure interne.
Tale sistema è integrato nei più generali assetti organizzativi, amministrativi e di governo societario adottati dal Gruppo e tiene in adeguata considerazione i modelli di riferimento e le *best practice* esistenti in ambito nazionale e internazionale. Il grado di integrazione del sistema, più in particolare, è misurato dal grado di omogeneità, interdipendenza ed integrazione dei suoi diversi attori e componenti.
In quest'ottica la Società integra le attività e procedure di controllo rese obbligatorie a seguito di interventi del legislatore ovvero di autorità tutorie con quelle adottate per scelte di politica gestionale, eventualmente ampliandone l'ambito di applicazione ove ritenuto necessario.
Pertanto, nel sistema integrato un ruolo di rilievo è offerto dai sistemi di organizzazione e controllo sviluppati in conformità ai disposti normativi del D. Lgs. 231/01 (responsabilità amministrativa degli enti), ivi inclusi il sistema di controllo relativo alla sicurezza, igiene e salute sul lavoro ai sensi del D. Lgs. 81/08, della L. 262/05 sulla tutela del risparmio (introduzione del ruolo del Dirigente Preposto ai documenti contabili e societari), della legge sulla "privacy" oltre che in riferimento a modelli organizzativi consolidati per il controllo in specifici ambiti quali la "qualità".
Il perseguimento di obiettivi di efficacia ed economicità del SCIGR nel suo complesso richiede pertanto una modalità che consenta una omogenea identificazione e valutazione dei rischi ed un approccio sinergico al disegno dei controlli nei diversi ambiti aziendali di applicazione.
Il SCIGR consente di ridurre l'impatto dei rischi sull'attività aziendale e fornisce rassicurazioni ragionevoli, ancorché non assolute, sul fatto che la Società ed il Gruppo nel suo complesso non risultino ostacolati nel raggiungimento dei propri obiettivi gestionali ovvero nello svolgimento ordinato e legittimo del proprio business da circostanze o elementi che possano essere ragionevolmente previsti, nella consapevolezza che nessun processo di controllo può, in termini assoluti, preservare dai rischi intrinseci all'attività imprenditoriale né dalla possibilità che violazioni fraudolente di leggi e regolamenti o delle procedure aziendali, errori umani o eventi straordinari possano procurare danni.

Il SCIGR, definito in base alle migliori prassi nazionali ed internazionali, si articola sui seguenti tre livelli di controllo:

- 1° livello: le funzioni operative identificano e valutano i rischi e definiscono specifiche azioni di trattamento per la loro gestione;
- 2° livello: le funzioni preposte al controllo dei rischi definiscono metodologie e strumenti per la gestione dei rischi e svolgono attività di monitoraggio dei rischi;
- 3° livello: la funzione di *Internal Audit* fornisce valutazioni indipendenti sull'intero SCIGR.

2. COORDINAMENTO TRA I SOGGETTI COINVOLTI NEL SISTEMA DI CONTROLLO INTERNO E GESTIONE DEI RISCHI

Il Sistema di Controllo Interno e di Gestione dei Rischi coinvolge, ciascuno per le proprie competenze, il Consiglio di Amministrazione, l'Amministratore Delegato, il Comitato Controllo e Rischi, il Collegio Sindacale, il Responsabile Internal Audit, l'Organismo di Vigilanza istituito ai sensi del Decreto Legislativo 8 giugno 2001, n. 231, il Dirigente Preposto e Risk Manager, e prevede - anche in linea con quanto raccomandato dal Codice di Corporate Governance - modalità di coordinamento tra detti soggetti, in relazione a ruoli e competenze in materia di Sistema di Controllo Interno e di Gestione dei Rischi, al fine di massimizzare l'efficienza complessiva del SCIGR, nel rispetto dei rispettivi ruoli e responsabilità, e ridurre duplicazioni di attività. Il Collegio Sindacale e il Comitato Controllo e Rischi si scambiano tempestivamente le informazioni rilevanti per l'espletamento dei relativi compiti. Il Presidente del Collegio Sindacale, o altro componente da lui designato, partecipano ai lavori del Comitato Controllo e Rischi.
Il Presidente del Collegio Sindacale, o altro Sindaco effettivo da questi designato, assiste altresì alle riunioni del Comitato Nomine e Remunerazione e del Comitato Operazioni con Parti Correlate. Possono in ogni caso assistere alle riunioni dei predetti Comitati endo-consiliari tutti i componenti del Collegio Sindacale.
Al fine di garantire un adeguato coordinamento tra i soggetti coinvolti nel SCIGR, la Società pone in essere:

- flussi informativi idonei e continui tra i soggetti coinvolti nel SCIGR,
- incontri ad hoc per la gestione di eventi o situazioni specifiche, necessari ad assicurare tempestività nel controllo delle esposizioni ai rischi e nella rilevazione di anomalie operative,
- incontri periodici per comunicare lo status del sistema di gestione dei rischi e pianificare le attività di verifica.

I 3 livelli di controllo, nel rispetto dei propri ruoli e responsabilità, comunicano, collaborano e si coordinano con l'obiettivo di massimizzare l'efficacia e l'efficienza dei sistemi di controllo e la creazione di valore sostenibile lungo tutta la catena del valore.

3. COMPITI RELATIVI AL SISTEMA DI CONTROLLO INTERNO E GESTIONE DEI RISCHI

3.1 Gli attori del Sistema di Controllo Interno e Gestione dei Rischi

La tabella che segue fornisce una sintesi schematica del quadro degli attori del SCIGR, identificandone il ruolo e le principali funzioni rispettivamente svolte ciascuno per le proprie competenze:

ORGANISMO	RUOLO NEL SISTEMA DI CONTROLLO INTERNO E GESTIONE DEI RISCHI				
	VALUTAZIONE	SUPERVISIONE	PROGETTAZIONE DEL SISTEMA	ATTUAZIONE E GESTIONE DEL SISTEMA	ESECUZIONE DEI CONTROLLI
Consiglio di Amministrazione	√		√	√	
Collegio Sindacale	√				
Organismo di Vigilanza D. Lgs. 231/01	√		√	√	√
Comitato Controllo e Rischi	√				
Amministratore Delegato		√	√	√	
Risk Manager – Livello 2°	√	√		√	
Comitato Rischi – Livello 2°		√			
Dirigente Preposto L. 262/05 – Livello 2°	√			√	√
Responsabile Servizio Prevenzione e Protezione- Livello 2°	√			√	√
Data Protection Officer – Livello 2°		√		√	√
Tax Risk Officer – Livello 2°	√	√		√	√
Cybersecurity Supervisor – Livello 2°	√			√	√
Responsabile Funzione Internal Audit – Livello 3°		√			
Internal Audit - Livello 3°					√
Responsabili operativi (Direttore Generale, management) - Livello 1°					√

3.2 Ruolo e responsabilità del Consiglio di Amministrazione

Il Consiglio di Amministrazione ("CdA"), nella sua qualità di organo di supervisione strategica, ha la responsabilità finale del SCIGR e ne valuta periodicamente l'adeguatezza e l'efficienza, promuovendo altresì a tutti i livelli aziendali una cultura che valorizzi la funzione del controllo.

In particolare, il CdA, con il supporto del Comitato Controllo e Rischi ("CCR"):

a) definisce le presenti linee di indirizzo allo scopo di ottenere che i principali rischi siano correttamente identificati nonché adeguatamente misurati, gestiti e monitorati e, in ultima analisi, verifica che i rischi assunti siano compatibili con gli obiettivi aziendali stabiliti;
b) valuta periodicamente, con cadenza almeno annuale, l'adeguatezza e l'efficacia del SCIGR avuto riguardo alle caratteristiche dell'impresa ed al profilo di rischio assunto;
c) approva, con cadenza almeno annuale, il piano di lavoro predisposto dal Responsabile della funzione *Internal Audit*, sentiti il Collegio Sindacale ("CdS") e l'Amministratore Delegato ("AD");

d) descrive, nella relazione sul governo societario, le principali caratteristiche del SCIGR, esprimendo la propria valutazione sull'adeguatezza dello stesso;
e) approva il Modello di Organizzazione, Gestione e Controllo ai sensi D. Lgs. 231/01;
f) valuta, sentito il CdS, i risultati esposti dai revisori legali o dalla società di revisione legale nella lettera di suggerimenti e nella relazione sulle questioni fondamentali emerse in sede di revisione legale, compresi i risultati esposti ai fini dell'attestazione della rendicontazione di sostenibilità;
g) approva le misure di implementazione del Modello Organizzativo NIS2, volte a prevenire i rischi di cybersecurity, ai sensi dell'art.23 del D. Lgs. 138/2024 (di seguito "Decreto NIS") come definite dall'Agenzia di Cybersicurezza Nazionale (ACN) tramite le proprie Determinazioni, tra cui la Determinazione ACN n.379907 del 19 dicembre 2025.

Ai fini di un corretto svolgimento dei compiti demandati alla sua responsabilità, il CdA si avvale del supporto di specifici organi preposti.

Pertanto, il CdA:
- istituisce il CCR attribuendogli funzioni consultive e propositive in relazione al SCIGR e nominandone i componenti;
- previo parere del CCR, nonché sentito in CdS:
    i. nomina e revoca, il Responsabile della funzione *Internal Audit* ("RIA"), inquadrandone l'attività da un punto di vista organizzativo, assicurandosi che quest'ultimo sia dotato di risorse adeguate all'espletamento delle proprie responsabilità e definendone la remunerazione coerentemente con le politiche aziendali;
    ii. nomina l'Organo di Vigilanza ai sensi D. Lgs. 231/01.

Il Cda effettua con cadenza triennale, e comunque in vista del rinnovo dello stesso, un'autovalutazione sulla dimensione, sulla composizione e sul concreto funzionamento propri e dei comitati interni.

3.3 Ruolo e responsabilità dell'Amministratore Delegato

L'Amministratore delegato ("AD") svolge il ruolo di amministratore incaricato del Sistema di Controllo Interno e di Gestione dei rischi.
L'AD ha la responsabilità di dare esecuzione alle presenti linee di indirizzo del SCIGR con il supporto del CCR e di assicurare che siano adottate tutte le azioni necessarie alla realizzazione del sistema.

In particolare, l'AD svolge i seguenti compiti:

a) cura l'identificazione e la gestione dinamica dei principali rischi aziendali, tenendo conto delle attività svolte nell'ambito del Gruppo, sottoponendoli periodicamente all'esame del CdA;
b) dà esecuzione alle linee di indirizzo del SCIGR definite dal CdA, curando la progettazione, realizzazione e gestione del SCIGR, verificandone costantemente l'adeguatezza e l'efficacia nonché curandone l'adeguamento alla dinamica delle condizioni operative e del panorama legislativo e regolamentare;
c) può chiedere alla funzione *Internal Audit* di svolgere verifiche su specifiche aree operative e sul rispetto delle regole e procedure interne nell'esecuzione di operazioni aziendali, dandone contestuale comunicazione al Presidente del CdA, al Presidente del CCR ed al Presidente del CdS;
d) riferisce tempestivamente al CCR in ordine a problematiche e criticità emerse nello svolgimento della propria attività o di cui abbia avuto comunque notizia, affinché il CCR possa prendere le opportune iniziative;
e) propone al CdA, previo parere del CCR, la nomina, la revoca e la remunerazione del RIA.

L'Amministratore Delegato partecipa al processo di condivisione verso il Consiglio di Amministrazione delle misure di mitigazione del rischio di cybersecurity, secondo quanto previsto dal Modello Organizzativo NIS2.

3.4 Ruolo e responsabilità del Responsabile Internal Audit

Il Responsabile Internal Audit ("RIA"), il quale non è responsabile di alcuna area operativa e dipende gerarchicamente dal CdA collocandosi in staff all'AD, ha le seguenti responsabilità:

a) verifica, sia in via continuativa sia in relazione a specifiche necessità e nel rispetto degli standard internazionali, l'operatività e l'idoneità del SCIGR attraverso un Piano di *Audit* approvato dal CdA e basato su un processo strutturato di analisi e prioritizzazione dei principali rischi;
b) predispone relazioni periodiche contenenti adeguate informazioni sulla propria attività, sulle modalità con cui viene condotta la gestione dei rischi nonché sul rispetto dei piani definiti per il loro contenimento; dette relazioni contengono una valutazione sull'idoneità del sistema di controllo interno e di gestione dei rischi;
c) predispone tempestivamente relazioni su eventi di particolare rilevanza;
d) trasmette le relazioni di cui ai punti b) e c) ai Presidenti del CdS, del CCR e del CdA nonché all'AD;
e) verifica, nell'ambito del Piano di *Audit* approvato dal CdA, l'affidabilità dei sistemi informativi inclusi i sistemi di rilevazione contabile.

Inoltre, con il supporto del Risk Manager, il RIA valuta e monitora i rischi legati al processo di rendicontazione della sostenibilità, ad esempio i rischi legati a: completezza/integrità dei dati; accuratezza dei risultati delle stime; disponibilità di dati sulla catena del valore a monte e/o a valle; tempistiche con cui le informazioni sono rese disponibili.
Nell'ambito dei propri compiti e responsabilità il RIA ha accesso diretto a tutte le informazioni utili per lo svolgimento del proprio incarico.
In particolare, il RIA opera attraverso una struttura organizzativa dedicata all'*Internal Audit* la quale svolge altresì un'attività di supporto all'AD nello svolgimento di verifiche su specifiche aree operative e sul rispetto di procedure e regole interne nello svolgimento delle operazioni gestionali.

Nell'ambito delle attività di controllo da svolgere sotto la supervisione del RIA, l'*Internal Audit* predispone un Piano di verifiche annuale ("Piano di *Audit*") da sottoporre all'esame del CCR e all'approvazione del CdA, e, su base almeno semestrale, una relazione da sottoporre al CdA, al CCR ed al CdS.
Su indicazione del Dirigente Preposto alla redazione dei documenti contabili societari ("DP"), cui risponde funzionalmente in relazione a questo tipo di attività, l'*Internal Audit* può eseguire le verifiche sul sistema dei controlli amministrativo-contabili previsti dalla L. 262/05.
Su indicazione dell'OdV, l'*Internal Audit* può eseguire le verifiche sul sistema dei controlli previsti dal Modello di Organizzazione, Gestione e Controllo di cui al D. Lgs. 231/01.
Inoltre, su indicazione dell'OdV, *l'Internal Audit* può eseguire le verifiche sul sistema dei controlli previsti dal D. Lsg. 138/2024, con riferimento alle misure di implementazione volte a prevenire i rischi di cybersecurity previste dal Decreto NIS e definite dall'Agenzia di Cybersicurezza Nazionale (ACN) tramite le proprie Determinazioni (ad esempio, Determinazione ACN n.379907 del 19 dicembre 2025).

L'*Internal Audit,* valuta periodicamente l'adeguatezza del *Tax Control Framework* in termini di disegno ed effettivo funzionamento attraverso valutazioni indipendenti.

3.5 Ruolo e responsabilità del Risk Manager

I compiti del Risk Manager sono i seguenti:

a) implementare, sviluppare e tenere costantemente aggiornato un sistema di identificazione, valutazione, gestione e monitoraggio dei rischi secondo i principi tipici dell'ERM;
b) supportare i responsabili di funzione ("risk owner") durante la fase di individuazione ("risk assessment") e di gestione dei rischi presidiati;
c) collaborare con i "risk owner" nello sviluppo di processi e procedure volti alla mitigazione del rischio nelle rispettive aree di competenza;
d) promuovere lo sviluppo di una cultura del rischio all'interno dell'organizzazione.

Al Risk Manager è dunque affidata la responsabilità di presidiare il processo di gestione dei rischi aziendali attraverso le metodologie tipiche dell'ERM proponendo, se necessario, agli attori del SCIGR interventi finalizzati all'adeguamento del sistema di controllo interno.

Con cadenza annuale il Risk Manager effettua una revisione critica della mappatura dei rischi e del sistema di gestione e monitoraggio degli stessi (ERM) e ne presenta i risultati all'AD, al CCR e al RIA. Egli informa inoltre, con cadenza semestrale, l'AD, il CCR, il CdS e l'ODV sull'attività di controllo dei rischi svolta.

3.6 Ruolo e responsabilità del Comitato Rischi

Il Comitato Rischi, composto da AD, RIA, Risk Manager, Direttore Generale e Direttore Amministrativo di Gruppo, ha il compito di supportare l'AD nello svolgimento del compito istituzionale consistente nell'individuazione dei principali rischi aziendali, specie di quelli emergenti per effetto dell'ingresso in nuove aree di attività e/o business ovvero legate ad evoluzioni della normativa generale, anche in materia fiscale, e di settore.

Pertanto, il Comitato Rischi affianca l'AD, tenuto conto che questo profilo non dedica la totalità del suo tempo alle funzioni svolte nell'ambito del SCIGR, per quanto riguarda l'aggiornamento e la manutenzione della mappa dei principali rischi aziendali definita all'inizio di ogni esercizio fiscale ed approvata dal CdA. Esso coadiuva gli organi sociali nel processo di individuazione di nuove aree di rischio e fornisce, laddove possibile ovvero consigliato per un carattere di particolare urgenza, una prima indicazione circa le azioni da porre in essere al fine di introdurre ovvero razionalizzare e/o migliorare i presidi tesi alla mitigazione dei rischi individuati.

3.7 Ruolo e responsabilità del Comitato Controllo e Rischi

Relativamente al SCIGR, il Comitato Controllo e Rischi ("CCR") ha il compito di supportare le decisioni e valutazioni del CdA con un'adeguata attività istruttoria, in modo che i principali rischi afferenti alla Società ed al Gruppo siano correttamente identificati nonché adeguatamente misurati, gestiti e monitorati, ed assiste per quanto di competenza il CdA nelle decisioni relative all'approvazione delle relazioni finanziarie periodiche.

In tale ambito il CCR:

a) supporta il CdA nell'espletamento dei compiti a quest'ultimo demandati in materia di controllo interno e di gestione dei rischi relativi:

    i. alla definizione delle linee di indirizzo del sistema di controllo interno e di gestione dei rischi in coerenza con le strategie della Società;
    ii. alla definizione del Modello Organizzativo NIS2 (Direttiva UE/2022/2555) di cui alla misura GV.RR (Responsabilità, Ruoli e correlati poteri) dell'Allegato I, Determinazione ACN n.379907 del 19 dicembre 2025, D.lgs. 138/2024 (cosiddetto "Decreto NIS");

iii. all' accertamento che i principali rischi aziendali siano identificati e gestiti in modo adeguato;
iv. alla nomina e revoca del responsabile della funzione "internal audit", assicurando che lo stesso sia dotato delle risorse adeguate all'espletamento delle proprie responsabilità, e su quelle inerenti la sua remunerazione, coerentemente con le politiche aziendali;
v. all' approvazione, con cadenza almeno annuale, del piano di lavoro predisposto dal responsabile della funzione "internal audit", sentiti il Collegio Sindacale e l'Amministratore Delegato;
vi. alla valutazione dell'opportunità di adottare misure per garantire l'efficacia e l'imparzialità di giudizio delle altre funzioni aziendali coinvolte nei controlli (quali le funzioni di risk management, di presidio del rischio legale e di non conformità e della funzione Internal Audit);
vii. all' attribuzione all'Organismo di Vigilanza delle funzioni di vigilanza ex art.6, comma 1, lettera b) del Decreto Legislativo n. 231/2001;
viii. alla valutazione, sentito il Collegio Sindacale, dei risultati esposti dal revisore legale nella eventuale lettera di suggerimenti e nella relazione sulle questioni fondamentali emerse in sede di revisione legale;
ix. alla descrizione, nella relazione sul governo societario, delle principali caratteristiche del sistema di controllo interno e di gestione dei rischi, esprimendo la propria valutazione sull'adeguatezza dello stesso.

b) valuta sentiti il DP, il revisore legale ed il CdS, il corretto utilizzo dei principi contabili e la loro omogeneità ai fini della redazione del bilancio consolidato e il corretto utilizzo degli standard applicabili ai fini della rendicontazione di sostenibilità;
c) valuta l'idoneità dell'informazione periodica, finanziaria e della rendicontazione di sostenibilità, a rappresentare correttamente il modello di business, le strategie della Società, l'impatto della sua attività e le performance conseguite;
d) esamina il contenuto della rendicontazione di sostenibilità rilevante ai fini del sistema di controllo interno e di gestione dei rischi;
e) 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;
f) esamina le relazioni periodiche, aventi per oggetto la valutazione del sistema di controllo interno e di gestione dei rischi, e quelle di particolare rilevanza predisposte dalla funzione "*internal audit*" e dalla funzione Tax Risk Management;
g) monitora l'autonomia, l'adeguatezza, l'efficacia e l'efficienza dell'operato della funzione di "*internal audit*" e della funzione di Tax Risk Management;
h) può chiedere alla funzione "*internal audit*" lo svolgimento di verifiche su specifiche aree operative, dandone contestuale comunicazione al Presidente del Cds;
i) svolge gli ulteriori compiti che gli vengono attribuiti dal CdA;
j) riferisce al CdA, almeno in occasione dell'approvazione della relazione finanziaria annuale e semestrale, sull'attività svolta nonché sull'adeguatezza del sistema di controllo interno e di gestione rischi rispetto alle caratteristiche dell'impresa ed al profilo di rischio assunto, nonché sulla sua efficacia;
k) valuta i rilievi che emergono dalle relazioni dell'Organismo di Vigilanza ai sensi della D. Lgs. n. 231/2001 e dalle indagini e dagli esami svolti da terzi;
l) valuta i rilievi che emergono dalle relazioni del Punto di Contatto di cui al D.lgs. 138/2024.

Con riferimento ai modelli di organizzazione e gestione previsti ai sensi del D. Lgs. 231/01, il CCR segue da vicino le relative attività di manutenzione ed aggiornamento acquisendo le informazioni a tale scopo sensibili.

Infine, il CCR formula pareri al Cda sulle regole della trasparenza e la correttezza sostanziale e procedurale delle operazioni con parti correlate e di quelle nelle quali un amministratore sia portatore di un interesse, in proprio o per conto di terzi, nonché svolge i compiti attribuiti al Comitato ai sensi del regolamento Consob recante disposizioni in materia di operazioni con parti correlate adottato con delibera n. 17221 del 12 marzo 2010 e successivamente modificato con delibera n. 17389 del 23 giugno 2010, n. 19925 del 22 marzo 2017 e n. 19974 del 27 aprile 2017, n. 21396 del 10 giugno 2020 e n. 21624 del 10 dicembre 2020, in particolare:

i. in ordine alle operazioni di «minore rilevanza», fermo restando l'assetto decisionale adottato dalla Società attraverso il conferimento di deleghe e poteri ed anteriormente all'approvazione delle operazioni, esprimere un motivato parere non vincolante sull'interesse della Società al compimento dell'operazione nonché sulla convenienza e sulla correttezza sostanziale delle relative condizioni;
ii. in ordine alle operazioni di «maggiore rilevanza», partecipare alla fase delle trattative e nella fase istruttoria attraverso la ricezione di un flusso informativo completo e tempestivo ed esprimere a beneficio del Consiglio un preventivo motivato parere favorevole circa l'interesse della Società al compimento dell'operazione in oggetto oltre che sulla convenienza e sulla correttezza sostanziale delle relative condizioni.

Ai lavori del CCR partecipa il Presidente del CdS o altro sindaco da lui designato; possono comunque partecipare anche gli altri sindaci.

3.8 Ruolo e responsabilità dell'Organo di Vigilanza ai sensi D. Lgs. 231/01

Il SCIGR è completato, per la parte relativa alla prevenzione del rischio di commissione di reati amministrativi e quindi al rispetto della *compliance*, dal Codice Etico e dal "Modello di Organizzazione, Gestione e Controllo" ai sensi del D. Lgs. 231/01 (di seguito anche "il Modello").

Il CdA nomina un Organismo di Vigilanza ("OdV") avente il compito di vigilare:

a) sull'osservanza delle prescrizioni del Modello, in relazione alle diverse tipologie di reati contemplate dal D. Lgs. 231/01 e dalle successive leggi che ne hanno esteso il campo di applicazione;
b) sull'efficacia del Modello in relazione alla struttura aziendale ed all'effettiva capacità di prevenire la commissione dei reati;
c) sull'opportunità dell'aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento dello stesso in relazione alle mutate condizioni aziendali e/o normative.

Per l'espletamento delle proprie funzioni il CdA conferisce all'OdV i seguenti poteri:

- di verificare l'efficienza e l'efficacia del Modello anche in termini di conformità tra le modalità operative adottate in concreto e i protocolli formalmente previsti dal Modello stesso;
- di verificare la persistenza nel tempo dei requisiti di efficacia e di efficienza del Modello;
- di promuovere l'aggiornamento del Modello, formulando, ove necessario, al Presidente del CdA le proposte per eventuali aggiornamenti e adeguamenti da realizzarsi mediante modifiche e/o integrazioni che si dovessero rendere necessarie in conseguenza di significative violazioni delle prescrizioni del Modello, significative modifiche dell'assetto organizzativo della Società e/o delle modalità di svolgimento delle attività d'impresa ovvero di intervenute variazioni normative;
- di segnalare tempestivamente al Presidente del CdA, per gli opportuni provvedimenti, le violazioni accertate del Modello che possano comportare l'insorgere di una responsabilità in capo alla Società;
- di promuovere e definire le iniziative per la diffusione del Modello, nonché per la formazione del personale e la sensibilizzazione dello stesso all'osservanza dei principi contenuti nel Modello;

- di promuovere e elaborare interventi di comunicazione e formazione sui contenuti del D. Lgs. 231/01, sugli impianti della normativa sull'attività della Società e sulle norme comportamentali;
- di fornire chiarimenti in merito al significato ed all'applicazione delle previsioni contenute nel Modello;
- di promuovere l'implementazione di un efficace canale di comunicazione interna per consentire l'invio di notizie rilevanti ai fini del D. Lgs. 231/2001, garantendo la tutela e riservatezza del segnalante;
- di formulare e sottoporre all'approvazione del CdA la previsione di spesa necessaria al corretto svolgimento dei compiti assegnati;
- di accedere liberamente presso qualsiasi sede o ufficio della Società - senza necessità di alcun consenso preventivo - al fine di richiedere informazioni, documentazione e dati ritenuti necessari per lo svolgimento dei compiti previsti dal D. Lgs. 231/01;
- di richiedere informazioni rilevanti a collaboratori, consulenti e collaboratori esterni alla Società, comunque denominati;
- di promuovere l'attivazione di eventuali procedimenti disciplinari in conseguenza di riscontrate violazioni del Modello.

L'OdV predispone un piano programmatico annuale delle attività che intende svolgere, inclusivo del programma di interventi di verifica dei protocolli operativi adottati, il quale viene portato a conoscenza del CdA.
L'OdV comunica in via continuativa le risultanze della propria attività al Presidente del CdA e all'AD.
Inoltre, con cadenza semestrale, l'OdV elabora un rendiconto della propria attività e fornisce al CdA ed al CdS un quadro completo delle attività svolte.
Qualora invitato, il Presidente dell'OdV ovvero, in caso di impedimento, un altro componente dell'OdV da questi indicato, può partecipare alle riunioni del CdS e del CCR.

3.9 Ruolo e responsabilità del Dirigente Preposto

Il Dirigente Preposto ("DP"), per effetto delle prescrizioni della L. 262/05, ha la responsabilità del sistema di controllo amministrativo-contabile.

In particolare, il DP deve:

a) attestare con dichiarazione scritta che gli atti e le comunicazioni della Società diffusi al mercato e relativi all'informativa contabile, anche infrannuale, siano corrispondenti a risultanze documentali, ai libri e alle scritture contabili;
b) predisporre adeguate procedure amministrative e contabili per la formazione del bilancio di esercizio e del bilancio consolidato, ovvero suggerire modifiche a quelle esistenti, nonché di ogni altra comunicazione di carattere finanziario;
c) attestare, congiuntamente all'AD, con apposita relazione allegata al bilancio di esercizio, alla relazione finanziaria semestrale ed al bilancio consolidato:

   i. l'adeguatezza, in relazione alle caratteristiche dell'impresa, e l'effettiva applicazione delle procedure amministrativo-contabili, nel corso del periodo di riferimento;
   ii. la corrispondenza dei documenti, cui l'attestazione si riferisce, alle risultanze dei libri e delle scritture contabili e la loro idoneità a fornire una rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria della Società e dell'insieme delle società del Gruppo incluse nel perimetro di consolidamento.

Le attività di verifica promosse dal DP consistono nell'analisi dei flussi interni rilevanti ai fini contabili, del corretto funzionamento del sistema dei controlli amministrativo-contabili, nell'esame e validazione delle procedure aziendali aventi impatto sul bilancio d'esercizio, sul

bilancio consolidato e sui documenti soggetti ad attestazione nonché sulla valutazione, mediante adeguato supporto tecnico, del ruolo dei sistemi informativi aziendali nell'assicurare l'adeguatezza di procedure e controlli.

Il DP riferisce al CdA sullo stato del sistema dei controlli interni "*over financial reporting*" in occasione dell'approvazione del bilancio e della relazione finanziaria semestrale.

Ai sensi del comma 5-ter dell'art. 154-bis del TUF il DP attesta che la Rendicontazione di Sostenibilità inclusa nella relazione sulla gestione sia stata redatta conformemente agli standard di rendicontazione applicati.

3.10 Ruolo e responsabilità del Responsabile del Servizio di Prevenzione e Protezione

Il Responsabile del Servizio di Prevenzione e Protezione ("RSPP"), figura prevista dal D.Lgs. 81/2008, provvede:

a) all'individuazione dei fattori di rischio, alla valutazione dei rischi e all'individuazione delle misure per la sicurezza e la salubrità degli ambienti di lavoro, nel rispetto della normativa vigente sulla base della specifica conoscenza dell'organizzazione aziendale;
b) ad elaborare, per quanto di competenza, le misure preventive e protettive e i sistemi di controllo di tali misure;
c) a sviluppare processi, procedure, criteri e metodi per ottenere la migliore gestione possibile del rischio per le varie attività aziendali;
d) a proporre i programmi di informazione e formazione dei lavoratori;
e) a partecipare alle consultazioni in materia di tutela della salute e sicurezza sul lavoro, nonché alla riunione periodica di cui all'articolo 35 del D.Lgs. 81/2008.

3.11 Ruolo e responsabilità del Data Protection Officer

Il Data Protection Officer ("DPO") è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

a) informare e fornire consulenza alle società del Gruppo Esprinet ed ai dipendenti che eseguono il trattamento di dati personali in merito agli obblighi derivanti dal Regolamento GDPR e da altre disposizioni nazionali o dell'Unione Europea relative alla protezione dei dati;
b) sorvegliare l'osservanza del Regolamento GDPR, di altre disposizioni nazionali o dell'Unione Europea relative alla protezione dei dati nonché alle politiche adottate dalle società del Gruppo Esprinet in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire un parere in merito alle eventuali valutazioni di impatto che dovessero essere predisposte e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento GDPR;
d) cooperare con il Garante per la Protezione dei Dati Personali;
e) fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
f) tenere il registro delle attività di trattamento sotto la responsabilità del titolare e attenendosi alle istruzioni impartite

I compiti del Data Protection Officer attengono all'insieme di tutti trattamenti di dati da parte delle società del Gruppo Esprinet.

3.12 Ruolo e responsabilità del Tax Risk Officer

Il Tax Risk Officer, che risponde direttamente al Chief Administration Officer, è incaricato di eseguire i seguenti compiti:

a) assicura la definizione, l'aggiornamento e la diffusione dei documenti che formano il sistema normativo interno relativo al Tax Control Framework ("TCF");
b) monitora, in coordinamento con la Funzione Administration e le altre funzioni preposte, la normativa tributaria e le evoluzioni dei requisiti di legge in ambito TCF, al fine di assicurare l'aggiornamento della Mappa dei Rischi Fiscali;
c) assicura, in collaborazione con i risk owner di processo, le attività di identificazione e misurazione dei rischi fiscali e la rilevazione dei controlli rilevanti a presidio di tali rischi;
d) collabora alla definizione del sistema dei controlli interni e delle procedure finalizzato alla prevenzione dei rischi fiscali;
e) assicura l'aggiornamento periodico della Mappa dei Rischi Fiscali;
f) predispone il piano di monitoraggio dei controlli di secondo livello;
g) garantisce lo svolgimento delle attività di monitoraggio ("Test of design" e "Test of effectiveness") dei controlli a presidio del rischio fiscale;
h) garantisce supporto ai risk owner di processo nell'identificazione e supervisione dei piani di azione messi in atto per rimediare a eventuali carenze emerse dalle attività di monitoraggio;
i) garantisce il coordinamento dei flussi informativi con le altre unità coinvolte nel processo;
j) assicura la predisposizione della reportistica prevista dal processo di Tax Risk Management verso i risk owner (funzioni operative), le altre funzioni di controllo, il CCR, il CdA;
k) cura, in raccordo con le altre funzioni aziendali competenti in materia di formazione, un'adeguata formazione in ambito di fiscalità finalizzata a far conseguire alle funzioni coinvolte la consapevolezza dei rischi fiscali collegati, nonché un aggiornamento su base continuativa del personale dipendente in relazione al TCF;
l) redige, con cadenza almeno annuale, la relazione - di cui all'articolo 4, comma 2, del decreto legislativo 5 agosto 2015, n. 128 per gli aspetti di propria competenza;
m) supporta il Responsabile della Funzione Administration, per gli aspetti di competenza inerenti al TCF, nelle interlocuzioni con l'Agenzia delle Entrate;
n) si coordina con le altre funzioni di controllo interno per l'acquisizione degli esiti delle verifiche effettuate nell'ambito del sistema di controllo interno;
o) mantiene i rapporti e partecipa costantemente al dialogo con l'Agenzia delle Entrate per gli aspetti inerenti al TCF anche con il supporto del Responsabile della Funzione Administration sia nelle fasi successive all'invio dell'istanza per l'adesione al regime di Adempimento Collaborativo ex D.Lgs. 128/2015, sia in fase di successiva ammissione al regime.

3.13 Ruolo e responsabilità del Cybersecurity Supervisor

Il Cybersecurity Supervisor, che risponde direttamente al Director Technology, è incaricato di eseguire i seguenti compiti:

a) effettuare l'analisi dei rischi di cybersicurezza, garantendone l'aggiornamento periodico e il monitoraggio costante;

b) curare la definizione, l'implementazione e il costante aggiornamento delle misure tecniche e organizzative volte a proteggere reti, dati e sistemi aziendali, garantendone la conformità ai requisiti normativi applicabili.

c) gestire e supervisionare l'elaborazione, l'efficacia e la revisione dei piani di risposta agli incidenti, assicurando il monitoraggio continuo e la tempestività delle azioni intraprese in caso di eventi avversi;

d) presidiare la gestione degli incidenti di sicurezza informatica, coordinando le attività di rilevazione, risposta e mitigazione e assicurando la tempestiva comunicazione all'Agenzia per la Cybersicurezza Nazionale;

e) valutare l'idoneità e l'adeguatezza dei fornitori sotto il profilo della sicurezza informatica e accertare il rispetto dei requisiti contrattuali stabiliti.

3.14 Ruolo e responsabilità del Collegio Sindacale

Il Collegio Sindacale ("Cds") svolge le tipiche attività di vigilanza previste dall'ordinamento nazionale accertando la conformità alla legge ed all'atto costitutivo e l'osservanza dei principi di corretta amministrazione.

Il CdS vigila inoltre:

a) 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;
b) sulle modalità di concreta attuazione delle regole di governo societario prevista da codici di comportamento redatti da società di gestione dei mercati regolamentati o da associazioni di categoria che la Società abbia dichiarato pubblicamente di avere recepito;
c) sull'adeguatezza delle disposizioni impartite dalla Società alle società controllate.

Nell'espletamento delle proprie attività il CdS può chiedere alla funzione Internal Audit di svolgere verifiche su specifiche aree operative od operazioni aziendali. Il CdS scambia tempestivamente con il CCR le informazioni rilevanti per l'espletamento dei rispettivi compiti e funzioni.

In qualità di Comitato per il Controllo Interno e la Revisione Contabile ("CCIRC"), come stabilito dall'art. 19 del D. Lgs. 39/2010, il CdS vigila su:

a) il processo di informativa finanziaria;
b) l'efficacia dei sistemi di controllo interno, di revisione interna, se applicabile, e di gestione del rischio;
c) la revisione legale dei conti annuali e dei conti consolidati;
d) l'indipendenza del revisore legale o della società di revisione legale, in particolare per quanto concerne la prestazione di servizi non di revisione all'ente sottoposto alla revisione legale dei conti.

Il revisore legale o la società di revisione legale presenta al CCIRC una relazione sulle questioni fondamentali emerse durante la revisione sulle carenze significative riscontrate nel sistema dei controlli interni riferiti al processo di informativa finanziaria. Essi inoltre devono confermare annualmente al CCIRC la propria indipendenza e gli eventuali servizi "non audit" forniti alle società del Gruppo e discutere periodicamente dei rischi relativi alla propria indipendenza nonché delle misure adottate per limitarli o neutralizzarli. Il CdS rileva la generale conformità alla legge della forma e del contenuto del bilancio, la corretta adozione dei principi contabili vigenti, la rispondenza del bilancio ai fatti e alle informazioni di cui il CdS sia venuto a conoscenza per effetto della partecipazione alle riunioni degli organi sociali, dell'esercizio dei suoi doveri di vigilanza e dei suoi poteri di ispezione e controllo.
Il CdS esprime un parere all'Assemblea degli azionisti sul conferimento e la revoca dell'incarico al revisore legale. Il CdS valuta, oltre che l'indipendenza del revisore legale, anche l'idoneità tecnica con riguardo all'organizzazione di quest'ultima rispetto all'ampiezza e complessità dell'incarico. Nell'espressione del parere suddetto il CdS tiene conto del compenso spettante alla società di revisione in relazione al piano di revisione presentato.

Ai sensi dell'articolo 10, comma 1, del Dlgs 125/2024, il CdS vigila sull'osservanza delle disposizioni in materia di sostenibilità e ne riferisce nella relazione annuale all'Assemblea. In quest'ambito, il CdS:

- verifica che il CdA valuti l'adeguatezza dell'assetto organizzativo della Società alle esigenze introdotte dalla normativa in materia di sostenibilità e, se necessario, provveda alle conseguenti modifiche;
- vigila sul processo di formazione del reporting di sostenibilità;

A tal fine, il CdS incontra la società di revisione incaricata dell'attestazione della rendicontazione di sostenibilità per uno "scambio di informazioni" sulla pianificazione delle relative attività, sul livello di estensione dei controlli alle società del gruppo, sul sistema di controllo interno e sui controlli svolti in vista del rilascio della *assurance*, anche in relazione alla presenza nel *reporting* di tutte le informazioni obbligatorie. Il CdS può altresì approfondire come siano state implementate le attività che devono essere svolte dal Dirigente Preposto per garantire la qualità dei dati inseriti nel *reporting* di sostenibilità. Il CdS vigila infine sul rispetto degli obblighi di pubblicità del *reporting*, introdotti dall'art. 6 del D.Lgs. 125/2024.

3.15 Ruolo e responsabilità del *management* e dei dipendenti

Il *management* ed i dipendenti del Gruppo, ciascuno in funzione delle proprie competenze e dei compiti rispettivamente loro affidati nell'ambito dell'organizzazione aziendale, devono contribuire ad assicurare un efficace funzionamento del SCIGR in quanto parte della loro responsabilità nel raggiungimento degli obiettivi, informando il proprio referente superiore in ordine alle carenze riscontrate.

Essi, pertanto, devono avere la necessaria conoscenza, preparazione e capacità per agire ed operare nell'ambito del SCIGR e deve essere loro consentito di adempiere ai compiti conseguenti al proprio ruolo ed assolvere alle proprie responsabilità. Questo implica, pertanto, il diritto ed il dovere di ogni singolo dipendente di avere piena conoscenza e comprensione della Società in cui opera e del Gruppo, dei meccanismi operativi, degli obiettivi, dei mercati in cui opera e dei rischi cui è quotidianamente esposto.

4. PRINCIPI GENERALI DI INDIRIZZO E CRITERI DI INDIVIDUAZIONE DEI PRINCIPALI RISCHI AZIENDALI

4.1 Il SCIGR consiste nell'insieme di regole, comportamenti, politiche, procedure e strutture organizzative che, globalmente considerati, consentono alla Società ed al Gruppo di:

a) facilitare l'efficienza e l'efficacia delle operazioni di gestione, consentendo adeguate reazioni ai rischi operativi, finanziari, legali, sociali, ambientali, di governance o di altra natura che possano essere di ostacolo nel raggiungimento degli obiettivi aziendali;
b) assicurare la qualità del sistema di *reporting* interno ed esterno, attraverso l'utilizzo di un idoneo sistema di registrazione e di processi che generino un flusso di informazioni significative e affidabili dentro e fuori l'organizzazione aziendale;
c) contribuire all'osservanza di norme e regolamenti così come delle procedure interne;
d) conseguire un adeguato grado di protezione dei beni aziendali da un uso inappropriato o fraudolento che possa in ultima analisi provocare perdite patrimoniali.

4.2 I controlli coinvolgono, con diversi ruoli e nell'ambito delle rispettive competenze, il CdA, l'AD, il CCR, il CdS, il RIA, il Risk Manager, il Tax Risk Officer, il Comitato Rischi, la funzione *Internal Audit*, il DP, l'OdV, gli organi di amministrazione e controllo delle società controllate e tutto il personale.
Oltre alle norme di riferimento, questi si attengono alle indicazioni ed ai principi contenuti nelle presenti Linee di Indirizzo.

4.3 Il SCIGR, pur nella consapevolezza che nessun processo di controllo può, in termini assoluti, preservare dai rischi intrinseci all'attività di impresa, né dalla possibilità che violazioni fraudolente di leggi e regolamenti o delle procedure aziendali, errori umani o eventi straordinari cagionino danni alla Società o al Gruppo, deve:

a) assicurare la necessaria separazione tra le funzioni operative e quelle di controllo, e pertanto essere strutturato in modo da evitare o ridurre al minimo le situazioni di conflitto di interesse nell'assegnazione delle rispettive competenze;
b) agevolare l'identificazione, la misurazione, la gestione ed il monitoraggio adeguato dei rischi assunti;
c) stabilire attività di controllo ad ogni livello operativo e individuare con chiarezza compiti e responsabilità, in particolare nelle fasi di supervisione e di intervento e correzione delle irregolarità riscontrate;
d) assicurare sistemi informativi affidabili e idonei processi di *reporting* ai diversi livelli ai quali sono attribuite funzioni di controllo;
e) garantire che le anomalie riscontrate siano tempestivamente portate a conoscenza di adeguati livelli dell'azienda;
f) consentire la registrazione di ogni fatto di gestione e, in particolare, di ogni operazione con adeguato grado di dettaglio.

4.4 Il SCIGR è soggetto ad esame e verifica periodici tenendo conto dell'evoluzione dell'operatività aziendale e del contesto di riferimento.

4.5 Il SCIGR deve consentire di fronteggiare con ragionevole tempestività le diverse tipologie di rischio cui risultano esposti, nel tempo, la Società ed il Gruppo (strategici, operativi, finanziari, fiscali, di *compliance* , sociali, ambientali, di governance).

4.6 Il SCIGR deve consentire di identificare, misurare e controllare il grado di esposizione della Società e del Gruppo ai diversi fattori di rischio, nonché di gestire l'esposizione complessiva secondo predefinite metodologie di *risk scoring*.

4.7 Il SCIGR deve prevedere, tra l'altro, procedure idonee ad evidenziare situazioni di anomalia che possano costituire indicatori di inefficienza anche dei sistemi di misurazione e controllo dei rischi.

4.8 Restano ferme, in coerenza con i principi generali di indirizzo del SCIGR:

a) le disposizioni di cui al Modello di Gestione, Organizzazione e Controllo ai sensi del D. Lgs. n. 231/2001;
b) l'insieme delle regole e procedure amministrative e contabili per la predisposizione dei documenti contabili e delle altre comunicazioni di carattere economico, patrimoniale e finanziario predisposte ai sensi di legge dal DP.
c) l'insieme delle regole, normative, policy e procedure che disciplinano il sistema volto a garantire la corretta gestione e il presidio dei rischi fiscali (*Tax Control Framework*).