MiT Sim S.p.A.

PARTE SPECIALE
MODELLO ORGANIZZATIVO 231

Storico delle revisioni

Data approvazione del C.d.A.	Versione	Evento
26 luglio 2022	V.1	Prima emanazione

Sommario

1. INTRODUZIONE

1.1 Struttura della Parte Speciale del Modello

Il Modello di organizzazione, gestione e controllo ex D. Lgs. 231/2001 (d'ora in poi "Modello 231" o il "Modello") di MIT SIM S.p.A. (d'ora in poi "MIT" o la "SIM") è costituito da:

- una "Parte Generale" che descrive i contenuti e gli impatti del D. Lgs. 231/2001 (d'ora in poi il "D. Lgs. 231/2001" o il "Decreto"), i principi base, gli obiettivi e l'approccio seguito ai fini dell'elaborazione dello stesso, i principi generali del sistema organizzativo e di controllo che costituiscono la base del Modello, il funzionamento dell'Organismo di Vigilanza e del sistema sanzionatorio-disciplinare e le modalità di adozione, diffusione, aggiornamento e applicazione dei contenuti del Modello;
- una "Parte Speciale" elaborata in base alle evidenze ottenute nella fase di mappatura delle attività a rischio che descrive nel dettaglio, con riferimento ad ogni singola "famiglia" di reati e singola fattispecie di reato individuata come applicabile alla SIM, i principi di comportamento generali e specifici che devono essere tenuti da tutti i destinatari del Modello Organizzativo (i complessivamente definiti "Destinatari" e singolarmente identificati, a titolo esemplificativo in "dipendenti" "collaboratori" ecc.) nello svolgimento delle attività sensibili ed i poteri di controllo e monitoraggio riservati all'Organismo di Vigilanza istituito ex art. 6, comma 1, lett. b) del Decreto (di seguito "Organismo di Vigilanza").

Nello specifico, la Parte Speciale ha lo scopo di:

- indicare le aree di rischio, i principi e presidi di controllo che i Destinatari sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza ed ai responsabili delle funzioni aziendali che con esso cooperano, gli strumenti esecutivi per esercitare le attività di controllo, monitoraggio e verifica.

Come indicato nella Parte Generale cui si rimanda, gli Amministratori della SIM con il supporto della Funzione Compliance, hanno svolto un'attività di analisi per l'identificazione dei reati previsti dal D. Lgs. 231/2001 applicabili a MIT e la valutazione del potenziale rischio di commissione per ciascuna famiglie di reato.

Le famiglie di reato ritenute rilevanti per MIT sono le seguenti (quelle escluse sono state ritenute "non applicabili" alla SIM):

- reati contro la Pubblica Amministrazione nella gestione dei finanziamenti pubblici (Art. 24);
- delitti informatici e trattamento illecito di dati (Art. 24 bis);
- delitti di criminalità organizzata (Art. 24 ter);
- reati nei rapporti con la Pubblica Amministrazione (Art. 25);
- reati societari (Art. 25 ter);
- delitti con finalità di terrorismo (Art. 25 quater);

- abuso di informazioni privilegiate (Art. 25 sexies);
- reati in tema di tutela della salute e sicurezza sul luogo di lavoro (Art. 25 septies);
- reati di ricettazione, riciclaggio e impiego denaro, beni o utilità, autoriciclaggio (Art. 25 octies);
- delitti in materia di violazione del diritto d'autore (Art. 25 novies);
- reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (Art. 25 decies);
- impiego di cittadini di paesi terzi il cui soggiorno è irregolare (Art. 25 duodecies);
- reati Tributari (Art. 25 quinquiesdecies).

Con riferimento alle famiglie di reato potenzialmente applicabili, sono stati, inoltre, individuati i processi ed attività di gestione/strumentali potenzialmente "sensibili" in conformità con quanto previsto dal D.Lgs. 231/2001, ovverosia quei processi nel cui ambito, in linea di principio, potrebbero verificarsi le condizioni e/o crearsi i mezzi per la commissione delle fattispecie di reato rilevanti ai fini del Decreto e che devono essere disciplinati tramite specifici presidi di controllo atti a prevenire il rischio relativo al compimento dei reati.

Tali processi sono di seguito identificati:

- antiriciclaggio;
- privacy:
- gestione e diffusione di informazioni privilegiate e di operazioni sul capitale;
- tenuta del registro insider;
- *internal dealing*;
- gestione delle operazioni personali;
- gestione delle operazioni con parti correlate;
- gestione dei conflitti di interesse;
- selezione e di gestione dei fornitori e degli *outsourcers*;
- negoziazione in conto proprio;
- collocamento degli strumenti finanziari;
- trasmissione ed esecuzione degli ordini;
- contabilità, bilancio, adempimenti amministrativi e aspetti fiscali.

Successivamente all'identificazione delle attività a Rischio-Reato e dei relativi processi di gestione/strumentali, MIT, sensibile alle esigenze di assicurare condizioni di correttezza e trasparenza nella conduzione degli affari e delle attività sociali e, in particolare, di prevenire la commissione di comportamenti illeciti rilevanti ai sensi del Decreto, ha deciso di integrare il proprio sistema di controllo interno, già conforme alle disposizioni di vigilanza in materia, con l'introduzione di specifici principi comportamentali e controlli a presidio delle aree potenziali di rischio individuate, riportati nelle singole sezioni del presente documento.

Nelle singole Parti Speciali sono pertanto elencati i riferimenti normativi aziendali che regolamentano le attività sensibili e che costituiscono il principale presidio alla commissione di reati, nonché le specifiche procedure operative, i principi comportamentali ed i controlli identificati a presidio delle aree di rischio.

Tali riferimenti normativi, principi comportamentali e controlli sono stati sottoposti all'esame dell'Amministratore Delegato e Direttore Generale responsabile direttamente della gestione delle attività individuate a rischio o per il tramite di terzi cui è stata affidata l'attività in outsourcing. Sempre all'Amministratore Delegato e Direttore Generale è affidato il compito di diffusione dell'intero Modello Organizzativo ai soggetti interessati, a seguito della relativa approvazione da parte del Consiglio d'Amministrazione della SIM.

La presente Parte Speciale del Modello Organizzativo, tiene conto dei servizi ed attività di investimento a cui la SIM è autorizzata ed alle recenti ulteriori autorizzazioni ricevute per quanto attiene, in particolare:

la prestazione dei servizi di investimento autorizzati (negoziazione in conto proprio, anche in contropartita diretta dei clienti, esecuzione ordini per conto dei clienti, ricezione e trasmissione di ordini e collocamento senza impegno irrevocabile nei confronti dell'Emittente), in Italia ed in tutti gli altri Paesi dell'Unione Europea, anche con la possibilità di detenere strumenti finanziari e disponibilità liquide della clientela;

- l'effettuazione delle negoziazioni nei mercati Euronext Growth Milan, Euronext Milan e Euronext MIV Milan e, più in generale, in tutti i mercati borsistici dove è aderente diretta;
- il riconoscimento della qualifica di EGA – Euronext Growth Advisor, da parte di Borsa Italiana.

Oltre all'impianto normativo, pertanto, ciascun principio comportamentale e ciascun controllo costituisce regola di condotta aziendale e forma parte essenziale del Modello 231 della SIM. Unitamente a tali principi, la SIM considera come parte integrante dei presidi e procedure di controllo la presenza e il rispetto di tutte le misure e le previsioni contenute nell'ambito della procedura di *whistleblowing.*

1.2 Principi generali di controllo

I principi generali di controllo delle attività, applicabili ed applicati a tutti i processi aziendali, adottati dalla SIM anche in quanto intermediario finanziario vigilato, sono i seguenti.

- Proporzionalità: le modalità di controllo tengono conto delle dimensioni, della struttura e della organizzazione della SIM. Le misure, i presidi procedurali, informativi e delle risorse umane dedicati ed i protocolli sono dimensionati alla sua operatività pur tenendo comunque conto delle evoluzioni che la SIM ha avuto sin dal suo avvio, in termini di espansione della sua operatività alla luce delle recenti autorizzazioni ricevute, come sopra illustrato.
- Segregazione delle attività: l'esercizio delle attività sensibili viene realizzato in stretta osservanza del principio generale di segregazione tra chi esegue, chi controlla e chi autorizza l'attività.
- Norme: la SIM adotta, mantiene ed applica disposizioni organizzative idonee a fornire almeno principi di riferimento generali per la regolamentazione dell'attività sensibile, in conformità alla normativa primaria e secondaria cui è assoggettata e alle prescrizioni del presente Modello Organizzativo;
- Poteri di firma e poteri autorizzativi: l'esercizio di poteri di firma e poteri autorizzativi interni avviene sulla base di regole formalizzate a tal fine introdotte;
- Tracciabilità: i soggetti dipendenti nonché i soggetti terzi (es. outsourcer), le funzioni interessate e/o i sistemi informativi utilizzati assicurano l'individuazione e la ricostruzione delle fonti, degli elementi informativi e dei controlli effettuati, che supportano la formazione e l'attuazione delle decisioni della SIM e le modalità di gestione delle risorse finanziarie.

I protocolli specifici sono declinati all'interno delle successive sezioni del presente documento.

La presente parte speciale si compone di n. 14 capitoli, ciascuno dedicato ad una specifica categoria di reati ai fini della responsabilità amministrativa degli enti che la Società ha analizzato in ragione delle caratteristiche della propria attività.

La struttura di ogni capitolo è caratterizzata dall'associazione tra singole fattispecie di reato, attività sensibili individuate dalla Società con riferimento – anche in via meramente potenziale - alle predette fattispecie di reato e normativa e protocolli specifici.

I protocolli generali e specifici sono stati definiti utilizzando come riferimento le Linee guida ABI, le linee guida di Confindustria e quelle adottate dalle principali associazioni di categoria.

2. REATI CONTRO LA PUBBLICA AMMINISTRAZIONE NELLA GESTIONE DEI FINANZIAMENTI PUBBLICI (ART. 24)

2.1 Identificazione dei reati applicabili alla SIM

In conformità a quanto previsto all' art. 6, comma 2, lett. a) del D. Lgs. 231/2001 sono state identificate le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati inclusi nel Decreto.

Nello specifico, si elencano di seguito le fattispecie di reato contemplate nel D. Lgs. 231/2001 all'art. 24 ritenute applicabili, anche se in via prudenziale, a MIT, in ragione delle attività svolte, rimandando all'Allegato 1 della Parte Generale per l'elencazione completa dei reati inclusi nella presente famiglia di reato:

Art. D. Lgs. 231/2001	**REATI PRESUPPOSTO (Codice Penale)**	
24 – Reati contro la Pubblica Amministrazione	Art. 316 bis	Malversazione a danno dello Stato
	Art. 316 ter	Indebita percezione di erogazioni a danno dello Stato
	Art. 640	Truffa aggravata a danno dello Stato
	Art. 640 bis	Truffa aggravata per il conseguimento di erogazioni pubbliche
	Art. 640 ter	Frode informatica

2.2 Identificazione delle attività e delle operazioni a rischio

Le attività che MIT ha individuato come sensibili, nell'ambito dei reati contro la Pubblica Amministrazione nella gestione dei finanziamenti pubblici, sono indicate in dettaglio nella Matrice delle Attività a Rischio-Reato conservata a cura della Società, unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

Alla luce dei presupposti applicativi del decreto, la SIM potrebbe essere considerata responsabile per i delitti contro la Pubblica Amministrazione commessi nel suo interesse o vantaggio da persone che rivestono funzioni di amministrazione, rappresentanza, ma anche da persone sottoposte alla loro direzione o vigilanza che svolgono attività esternalizzate.

Relativamente ai reati di Malversazione a danno dello stato e Indebita percezione di erogazioni pubbliche, tali ipotesi si configurano nel caso in cui, dopo avere ricevuto finanziamenti o contributi da parte dello Stato italiano o dell'Unione Europea (quale ad esempio l'ottenimento di bonus o contributi fiscali per la quotazione), non si proceda all'utilizzo delle somme ottenute per gli scopi cui erano destinate (la condotta, infatti, consiste nell'avere distratto, anche

parzialmente, la somma ottenuta o riconosciuta, senza che rilevi che l'attività programmata si sia comunque svolta) oppure nel caso in cui per l'ottenimento del contributo o del bonus fiscale si utilizzi o si presentino dichiarazioni o documenti falsi o attestanti informazioni, fatti, circostanze non vere o nell'omissione di informazioni dovute.

Tenuto conto che il momento consumativo del reato coincide con la fase esecutiva, il reato stesso può configurarsi anche con riferimento a finanziamenti o crediti di imposta già ottenuti in passato e che ora non vengano destinati alle finalità per cui erano stati erogati.

Relativamente ai reati di Truffa aggravata a danno dello Stato e Truffa aggravata per il conseguimento di erogazioni pubbliche si configurano nel caso in cui, per realizzare un ingiusto profitto, siano posti in essere degli artifici o raggiri tali da indurre in errore e da arrecare un danno allo Stato o ad altro ente pubblico, oppure nel caso in cui la truffa sia posta in essere per conseguire indebitamente erogazioni pubbliche, ad esempio, per il tramite dell'ottenimento di un crediti di imposta non dovuto oppure mediante l'escussione di una garanzia contro-garantita da un soggetto pubblico (Confidi o Cassa Depositi e Prestiti) nell'ambito di una obbligazione garantita emessa da un soggetto emittente assistito da parte della SIM. Essa può realizzarsi nel caso in cui si pongano in essere artifici o raggiri, ad esempio comunicando dati non veri o predisponendo una documentazione falsa, per ottenere finanziamenti pubblici.

Relativamente al reato di Frode Informatica, tale fattispecie si configura nel caso in cui, alterando il funzionamento di un sistema informatico o telematico o manipolando i dati in esso contenuti, si ottenga un ingiusto profitto arrecando danni a terzi. In concreto, può integrarsi il reato in esame qualora, una volta ottenuto il finanziamento, venisse violato il sistema informatico al fine di inserire un importo relativo ai finanziamenti superiore a quello ottenuto legittimamente.

Le attività individuate quali rilevanti per la SIM sono:

- produzione di documenti o dichiarazioni necessarie per l'ottenimento di contributi pubblici o crediti di imposta o altri bonus o benefici fiscali non veritieri o alterati;
- utilizzo improprio delle somme contributive ottenute rispetto allo scopo per cui erano state destinate;
- utilizzo improprio di sistema informatico della Pubblica Amministrazione per la gestione dei finanziamenti pubblici.

Attraverso l'individuazione delle attività esposte al rischio di reato ("attività sensibili") e la strutturazione di un sistema di controllo interno volto alla prevenzione di tali rischi, MIT intende:

- da un lato, determinare una piena consapevolezza in tutti coloro che operano in nome e per conto di MIT di poter incorrere in un illecito passibile di sanzione e la cui commissione è fortemente censurata dalla SIM, in quanto sempre contraria ai suoi interessi anche quando, apparentemente, essa potrebbe trarne un vantaggio economico immediato;
- dall'altro, in virtù di un monitoraggio costante delle attività, consentire di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

2.3 Principi specifici di comportamento

Coerentemente con i principi di cui alla Parte Generale del Modello Organizzativo ex D.Lgs. 231/2001 e del Codice Etico adottati dalla SIM, nello svolgimento delle attività sensibili sopra

citate tutti i Destinatari del Modello sono tenuti ad osservare i seguenti principi di comportamento:

- astenersi da qualsiasi condotta che possa compromettere la veridicità delle informazioni contenute nella documentazione o nelle dichiarazioni fornite alla Pubblica Amministrazione per l'ottenimento di contribuzioni;
- osservare il divieto di accedere in maniera non autorizzata ai sistemi informativi utilizzati dalla Pubblica Amministrazione o da altre Istituzioni Pubbliche, di alterarne in qualsiasi modo il funzionamento o di intervenire con qualsiasi modalità cui non si abbia diritto su dati, informazioni o programmi per ottenere e/o modificare indebitamente informazioni a vantaggio della SIM o di terzi;
- rispettare il divieto di richiedere e/o di utilizzare finanziamenti, contributi, crediti di imposta, mutui agevolati o altre erogazioni dello stesso tipo concessi o erogati dallo Stato, dalla Pubblica Amministrazione, da altri enti e/o Istituzioni pubbliche nazionali o comunitarie o da altri organismi di diritto internazionale, mediante la presentazione di dichiarazioni o di documenti falsi o attraverso l'omissione di informazioni dovute.

2.4 Procedure di controllo

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito l'elenco dei riferimenti normativi interni e delle procedure operative adottate dalla Società all'interno dei quali la Società ha definito i presidi di controllo a prevenzione della commissione dei reati in oggetto:

- Codice Etico;
- Regolamentazione privacy;
- Procedura relativa al collocamento degli strumenti finanziari;
- Memorandum sistema controllo di gestione.

3. DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI (ART. 24 bis)

3.1 Identificazione dei reati applicabili alla SIM

In conformità a quanto previsto all' art. 6, comma 2, lett. a) del D. Lgs. 231/2001 sono state identificate le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati inclusi nel Decreto.

Nello specifico, si elencano di seguito le fattispecie di reato contemplate nel D. Lgs. 231/2001 all'art. 24 bis ritenute applicabili, anche se in via prudenziale, a MIT, in ragione delle attività svolte, rimandando all'Allegato 1 della Parte Generale per l'elencazione completa dei reati inclusi nella presente famiglia di reato:

Art. D. Lgs. 231/2001	**REATI PRESUPPOSTO (Codice Penale)**	
24 bis – Delitti informatici e trattamento illecito di dati	Art. 491 bis	Falsità riguardanti un documento informatico
	Art. 615 ter	Accesso abusivo ad un sistema informatico o telematico
	Art. 615 quater	Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici
	Art. 635 bis	Danneggiamento di informazioni, dati e programmi informatici
	Art. 635 ter	Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità
	Art. 635 quater	Danneggiamento di sistemi informatici o telematici
	Art. 635 quinquies	Danneggiamento di sistemi informatici o telematici di pubblica utilità

3.2 Identificazione delle attività e delle operazioni a rischio

Le attività che MIT ha individuato come sensibili, nell'ambito dei delitti informatici, sono indicate in dettaglio nella Matrice delle Attività a Rischio-Reato conservata a cura della Società, unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

Alla luce dei presupposti applicativi del decreto, la SIM potrebbe essere considerata responsabile per i delitti informatici commessi nel suo interesse o vantaggio da persone che rivestono funzioni di amministrazione, rappresentanza, ma anche da persone sottoposte alla loro direzione o vigilanza che svolgono attività esternalizzate.

Le tipologie di reato informatico si riferiscono a una molteplicità di condotte criminose in cui un sistema informatico risulta, in alcuni casi, obiettivo stesso della condotta e, in altri, lo strumento attraverso cui l'autore intende realizzare altre fattispecie penalmente rilevanti. Nell'ambito dei sistemi informativi e contabili della SIM ve ne sono diversi che sono infatti utilizzati nell'ambito della prestazione dei servizi ed attività di investimento a cui è autorizzata. Si tratta, in particolare:

- di una apposita piattaforma fornita da un provider esterno che ha come finalità quella di consentire alla SIM di poter svolgere tutte le attività di *trading, post trading* e di controllo delle attività di *specialist* e per quelle relative alla prestazione dei servizi di investimento, che dialoga con le soluzioni informative che sono fornite dall'*outsourcer* a cui è affidato lo svolgimento delle attività amministrative e contabili;
- piattaforma per la postazione di trading (Bloomberg);
- di un applicativo per analizzare l'operatività ed individuare e segnalare alla competente Autorità di Vigilanza eventuali operazioni sospette ai fini del *market abuse*;
- di un applicativo per poter accedere alla consultazione della contabilità societaria e di prodotto ed ai dati relativi alle attività amministrative (*back office*) per la produzione delle segnalazioni nei confronti delle competenti Autorità di Vigilanza.

Le attività individuate quali rilevanti per la SIM sono:

- accesso ai sistemi informatici di terze parti;
- falsificazione di documenti informatici relativi, ad esempio, a rendicontazione in formato elettronico di attività e/o a attestazioni elettroniche di qualifiche o requisiti della SIM;
- acquisizione, detenzione e gestione abusiva di credenziali di accesso (password) a sistemi di terze parti.

Attraverso l'individuazione delle attività esposte al rischio di reato ("attività sensibili") e la strutturazione di un sistema di controllo interno volto alla prevenzione di tali rischi, MIT intende:

- da un lato, determinare una piena consapevolezza in tutti coloro che operano in nome e per conto di MIT di poter incorrere in un illecito passibile di sanzione e la cui commissione è fortemente censurata dalla SIM, in quanto sempre contraria ai suoi interessi anche quando, apparentemente, essa potrebbe trarne un vantaggio economico immediato;
- dall'altro, in virtù di un monitoraggio costante delle attività, consentire di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

3.3 Principi specifici di comportamento

Coerentemente con i principi di cui alla Parte Generale del Modello Organizzativo ex D.Lgs. 231/2001 e del Codice Etico adottati dalla SIM, nello svolgimento delle attività sensibili sopra citate tutti i Destinatari del Modello sono tenuti ad osservare i seguenti principi di comportamento:

- astenersi da qualsiasi condotta che possa compromettere la riservatezza e integrità delle informazioni e dei dati della SIM ed, in particolare, premurarsi di non lasciare incustoditi i propri sistemi informatici e bloccarli, qualora ci si allontani dalla propria postazione di

lavoro, con i codici di accesso e di spegnere il computer e gli eventuali altri dispositivi al termine della giornata lavorativa;

- astenersi da qualsiasi condotta diretta a superare o aggirare le protezioni del sistema informatico aziendale di terze parti o da cartelle aziendali protette da password;
- conservare i codici identificativi assegnati, astenendosi dal comunicarli a terzi, i quali, venendone in possesso, potrebbero accedere abusivamente a dati aziendali riservati od utilizzare le credenziali di accesso per forzare sistemi informativi di terze parti;
- astenersi dall'installare programmi non autorizzati.

3.4 Procedure di controllo

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito ulteriori presidi di controllo operativi a prevenzione della commissione dei reati, con particolare riferimento ai principali processi strumentali a presidio delle aree in oggetto tramite:

- installazione, manutenzione, aggiornamento o gestione di *software* di soggetti pubblici o forniti da terzi per conto dei soggetti pubblici;
- gestione degli accessi logici ai dati e ai sistemi ed alle piattaforme informatiche di soggetti terzi di cui si dispone della licenza d'uso;
- gestione dei *backup* della posta e dell'archivio dati;
- gestione della sicurezza della rete;
- gestione dei *software*, apparecchiature, dispositivi o programmi informatici (*change management);*
- gestione della sicurezza fisica.

I Destinatari, nello svolgimento delle attività di loro competenza, devono: **[da verificare alla luce delle linee guida del nuovo outsourcer IT]**

- utilizzare le risorse informatiche assegnate esclusivamente per l'espletamento della propria attività;
- utilizzare gli strumenti aziendali nel rispetto delle procedure interne predefinite;
- custodire accuratamente le proprie credenziali di accesso ai sistemi informativi propri o piattaforme informatiche di terzi e aggiornare periodicamente le password, evitando che terzi soggetti possano venirne a conoscenza;
- utilizzare beni protetti dalla normativa sul diritto d'autore nel rispetto delle regole ivi previste;
- limitare la navigazione in internet e l'utilizzo della posta elettronica attraverso i sistemi informativi aziendali alle sole attività lavorative.

Il Responsabile Information Technology (in outsourcing) deve:

- verificare la sicurezza della rete e dei sistemi informativi aziendali e tutelare la sicurezza dei dati;
- identificare le potenziali vulnerabilità nel sistema dei controlli informatici;
- valutare la corretta implementazione tecnica del sistema "deleghe e poteri" aziendale a livello di sistemi informativi ed abilitazioni utente al fine di rendere possibile la corretta segregazione dei compiti;
- garantire, sui diversi applicativi aziendali, l'applicazione delle regole atte ad assicurare l'aggiornamento delle password dei singoli utenti;

- installare a tutti gli utenti esclusivamente software originali, debitamente autorizzati e licenziati;
- monitorare l'infrastruttura tecnologica al fine di garantirne la manutenzione e la sicurezza fisica;
- effettuare le attività di backup e provvedere al corretto mantenimento dei file di log generati dai sistemi;
- garantire la manutenzione software e hardware dei sistemi e un processo di change management segregato;
- vigilare sulla corretta applicazione di tutti gli accorgimenti ritenuti necessari al fine di fronteggiare, nello specifico, i delitti informatici e il trattamento dei dati suggerendo ogni più opportuno adeguamento. Inoltre, le attività svolte da parte di fornitori terzi in materia di: o networking; o gestione applicativi; o gestione sistemi hardware devono rispettare i principi e le regole aziendali, al fine di tutelare la sicurezza dei dati ed il corretto accesso da parte dei soggetti ai sistemi applicativi ed infrastrutturali.

È fatto esplicito divieto di:

- utilizzare le risorse informatiche (es. personal computer fissi o portatili, dispositivi di memorizzazione portatile ecc.) assegnate da MIT per finalità diverse da quelle lavorative;
- porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso a sistemi informativi altrui con l'obiettivo di: o acquisire abusivamente informazioni contenute nei suddetti sistemi informativi; o danneggiare, distruggere dati contenuti nei suddetti sistemi informativi; o utilizzare abusivamente codici d'accesso a sistemi informatici e telematici nonché procedere alla diffusione degli stessi;
- porre in essere condotte miranti alla distruzione o all'alterazione dei documenti informatici aventi finalità probatoria ai sensi del D.Lgs. 231/2001;
- utilizzare o installare programmi diversi da quelli autorizzati dal Responsabile Information Technology o per i quali si è in possesso di una apposita licenza d'uso;
- effettuare download illegali o trasmettere a soggetti terzi contenuti protetti dal diritto d'autore;
- accedere ad aree riservate (quali server rooms, locali tecnici, ecc.) senza idonea autorizzazione, temporanea o permanente;
- aggirare o tentare di aggirare i meccanismi di sicurezza aziendali (antivirus, firewall, proxy server, ecc.);
- lasciare il proprio personal computer o altri dispositivi di memorizzazione portatile incustoditi e senza protezione;
- rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale o anche ad altri siti/sistemi;
- detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche.

E' garantito un accesso personale all'archivio elettronico della SIM; gli Amministratori, i dipendenti ed i collaboratori di MIT sono tenuti ad archiviare tutta la documentazione rilevante e comprovante la propria attività nelle cartelle appositamente assegnate dell'archivio societario.

A ciascun dipendente e ad ogni collaboratore che ne abbia necessità, ai fini dello svolgimento dell'attività lavorativa, è attribuito un indirizzo di posta elettronica aziendale individuale, configurato come segue: nome.cognome@MITsim.it o nome funzione@MITsim.it.

- Utilizzando gli indirizzi di posta elettronica aziendale e l'archivio, l'Amministratore o l'outsourcer è a conoscenza e consapevole che:

- tutti i messaggi in entrata e in uscita dagli indirizzi di posta elettronica aziendale e i file archiviati nell'archivio societario sono di proprietà della SIM;
- il messaggio di posta elettronica aziendale si configura come corrispondenza aperta che potrebbe essere letto da chiunque durante il suo percorso sulla rete internet fino al destinatario nonché dagli addetti IT (consulenti esterni) sul server aziendale che gestisce il servizio stesso;
- l'uso degli indirizzi di posta elettronica aziendale è ammesso esclusivamente per motivi attinenti all'attività lavorativa; l'uso per motivi personali è pertanto espressamente vietato. Nessuna aspettativa di tutela del proprio diritto alla privacy, relativa ai messaggi di posta elettronica in entrata ed in uscita utilizzando l'indirizzo aziendale, potrà, dunque, essere pretesa;
- il messaggio di posta elettronica potrebbe essere letto da destinatari diversi da quelli a cui era diretto, e ciò potrebbe determinare danni anche gravi alla SIM;
- i messaggi di posta elettronica spediti potrebbero non essere recapitati, essere distrutti o subire ritardi;
- le comunicazioni di posta elettronica sono considerate a tutti gli effetti posta in partenza e pertanto gli utenti dovranno verificare quanto scritto ed evitare di impegnare la SIM oltre le proprie deleghe.

Con specifico riferimento all'uso della posta elettronica aziendale, sia con l'esterno che all'interno della SIM, non è consentito:

- utilizzare gli indirizzi di posta elettronica aziendale per inviare o ricevere messaggi a carattere personale;
- utilizzare gli indirizzi di posta elettronica contenenti il dominio della SIM (@MITsim.it) per iscriversi in qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta della SIM;
- utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni alla SIM, informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte;
- creare, archiviare o spedire, anche all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) in nessun modo connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto utilizzando l'indirizzo aziendale;
- inviare, tramite la posta elettronica, anche all'interno della rete aziendale, alcun materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico;
- inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap. Qualora siano

ricevuti messaggi aventi tali contenuti, è tenuto a cancellarli immediatamente e a darne comunicazione tempestiva a Segreteria di Direzione che ne farà notifica al Responsabile IT e all'outsourcer dei servizi IT;
- utilizzare la posta elettronica aziendale in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248);
- inviare a indirizzi di posta elettronica privata, senza preventiva autorizzazione da parte dell'Amministratore Delegato e Direttore Generale, e_mail con allegati documenti aziendali od, anche senza allegati, e_mail di contenuto attinente all'attività lavorativa.

La perdita del PC portatile o di qualsiasi altro dispositivo informatico e/o di comunicazione (cellulare, tablet, ecc.), ancorché personali può provocare la perdita di informazioni importanti per la SIM e quindi costituisce sempre un danno economico per la stessa. Si richiede, quindi, particolare diligenza nel salvataggio dei file rilevanti ai fini della continuità dell'attività e nella custodia dei dispositivi elettronici in dotazione. OK.

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito l'elenco dei riferimenti normativi interni e delle procedure operative adottate dalla Società all'interno dei quali la Società ha definito i presidi di controllo a prevenzione della commissione dei reati in oggetto:

- Codice Etico;
- Regolamentazione privacy.

4. DELITTI DI CRIMINALITA' ORGANIZZATA (Art. 24 ter)

4.1 Identificazione dei reati applicabili alla SIM

In conformità a quanto previsto all' art. 6, comma 2, lett. a) del D. Lgs. 231/2001 sono state identificate le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati inclusi nel Decreto.

Nello specifico, si elencano di seguito le fattispecie di reato contemplate nel D. Lgs. 231/2001 all' art. 24 ter ritenute applicabili, anche se in via prudenziale, a MIT, in ragione delle attività svolte, rimandando all'Allegato 1 della Parte Generale per l'elencazione completa dei reati inclusi nella presente famiglia di reato:

Art. D. Lgs. 231/2001	**REATI PRESUPPOSTO (Codice Penale)**		
art. 24 ter: delitti di criminalità organizzata	Codice penale	art. 377 bis	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria
		art. 378	Favoreggiamento personale
		art. 416	Associazione per delinquere
		art. 416 bis	Associazioni di tipo mafioso anche straniere

4.2 Identificazione delle attività e delle operazioni a rischio

Le analisi condotte hanno portato a considerare teoricamente ravvisabile un Rischio-Reato in relazione all'evenienza che la SIM, nell'ambito delle proprie attività operative, possa indirettamente interagire con controparti a rischio potenzialmente riconducibili ad associazioni criminali e/o con finalità terroristiche.

In tale contesto la SIM ha, quindi, individuato come sensibili le attività di seguito riepilogate, indicate in dettaglio nella Matrice delle Attività a Rischio-Reato conservata a cura della SIM, alla quale si rimanda anche per esemplificazioni di potenziali modalità e finalità di realizzazione della condotta illecita:

- selezione, negoziazione, stipula ed esecuzione dei contratti con fornitori terzi di servizi o consulenze o collaborazioni;
- servizio di negoziazione in conto proprio, anche nell'ambito delle attività di operatore specialista;
- collocamento degli strumenti finanziari;
- trasmissione ed esecuzione degli ordini;
- attività di Euronext Global Advisory (EGA).

4.3 Principi specifici di comportamento

Coerentemente con i principi di cui alla Parte Generale del Modello Organizzativo ex D.Lgs. 231/2001 e del Codice Etico adottati dalla SIM, nello svolgimento delle attività sensibili sopra citate tutti i Destinatari del Modello sono tenuti ad osservare i seguenti principi di comportamento.

I reati di criminalità in senso lato trovano primario presidio nei principi del Codice Etico, nel sistema di deleghe e poteri nonché nel Modello nel suo complesso, che esplicitano principi e regole volte a prevenire il rischio che possa essere costituita un'associazione per delinquere all'interno della SIM.

Con specifico riferimento alle attività aziendali individuate come potenzialmente rilevanti, è fatto obbligo ai Destinatari del Modello di:

- assicurare un'approfondita conoscenza dei soggetti terzi con i quali vengono instaurati rapporti nell'esercizio del business della SIM, tra cui a titolo esemplificativo, potenziali società emittenti nei confronti delle quali la SIM presta le sue attività di Advisor (EGA) in sede di ammissione e in fase successiva all'ammissione alla quotazione; nell'ambito delle attività di collocamento (in fase di IPO, private placement o come aderente a consorzi di collocamento organizzati da soggetti terzi) prestato in favore di controparti qualificate o clienti professionali; oppure, in via residuale, nell'ambito dell'esecuzione degli ordini dei clienti (anche in contropartita diretta dei medesimi) con possibilità di detenere strumenti finanziari o disponibilità liquide dei medesimi;
- assicurare un'approfondita conoscenza dei soggetti terzi beneficiari di atti di disposizione del patrimonio della SIM;
- monitorare costantemente i flussi di denaro in entrata e in uscita;
- non effettuare alcuna operazione che possa presentare carattere anomalo per tipologia o oggetto ovvero che possa determinare l'instaurazione o il mantenimento di rapporti che presentino profili di anomalia dal punto di vista dell'affidabilità e/o della reputazione delle controparti;
- non riconoscere compensi in favore dei broker, consulenti, fornitori, *outsourcer* che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere, al servizio o attività da prestare e alle prassi vigenti in ambito locale;
- non selezionare personale i cui requisiti e la cui affidabilità non sia stata adeguatamente esaminata, compatibilmente con la legislazione vigente.

MIT, al fine di assicurare il corretto adempimento degli obblighi sopra descritti:

- si dota di un'adeguata organizzazione amministrativa e di un adeguato sistema di controlli interni, proporzionati alle dimensioni, alla natura e alle caratteristiche operative dell'impresa, volti a presidiare i rischi legati ai reati in oggetto;
- assicura che i Destinatari del Modello, in relazione alle proprie aree di responsabilità, siano sempre periodicamente aggiornati sulle procedure aziendali adottate per la prevenzione dei reati qui considerati.

4.4 Procedure di controllo

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito ulteriori presidi di controllo operativi a prevenzione della commissione dei reati in oggetto, con particolare riferimento ai principali processi strumentali a presidio delle aree in oggetto.

Essendo i reati in oggetto spesso propedeutici alla commissione di altri reati già contemplati nel presente Modello, si ritiene che i presidi già previsti in relazione alle ulteriori famiglie di reato applicabili siano utili per prevenire anche tali fattispecie di reato.

In ogni caso, per ciascuna delle Attività Sensibili, devono essere previste specifiche procedure, in forza delle quali:

- la scelta di collaboratori esterni avvenga sulla base di requisiti di professionalità, indipendenza e competenza ed in riferimento a essi sia motivata la scelta;
- non vengano instaurati rapporti contrattuali con controparti di cui non siano state raccolte tutte le informazioni, documenti e dati necessari e previsti nell'ambito delle procedure interne di cui la SIM è dotata;
- non siano corrisposti compensi, provvigioni o commissioni a terzi ed in particolare a *broker*, consulenti, collaboratori, fornitori in misura non congrua rispetto alle prestazioni rese alla SIM e non conformi all'incarico conferito, da valutare in base a criteri di ragionevolezza e in riferimento alle condizioni o prassi esistenti sul mercato o determinate da apposite tariffe.

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito l'elenco dei riferimenti normativi interni e delle procedure operative adottate dalla Società all'interno dei quali la Società ha definito i presidi di controllo a prevenzione della commissione dei reati in oggetto:

- Codice Etico;
- Tutte le procedure operative aziendali.

5. REATI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE (ART. 25)

5.1 Identificazione dei reati applicabili alla SIM

In conformità a quanto previsto all' art. 6, comma 2, lett. a) del D. Lgs. 231/2001 sono state identificate le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati inclusi nel Decreto.

Nello specifico, si elencano di seguito le fattispecie di reato contemplate nel D. Lgs. 231/2001 all' art. 25 ritenute applicabili, anche se in via prudenziale, a MIT, in ragione delle attività svolte, rimandando all'Allegato 1 della Parte Generale per l'elencazione completa dei reati inclusi nella presente famiglia di reato:

Art. D. Lgs. 231/2001	**REATI PRESUPPOSTO (Codice Penale)**	
Art. 25 – Reati nei rapporti con la Pubblica Amministrazione	art. 318	Corruzione per l'esercizio della funzione
	art. 319	Corruzione per un atto contrario ai doveri di ufficio
	art. 319 bis	Circostanze aggravanti
	art. 319 ter	Corruzione in atti giudiziari
	art. 319 quater	Induzione indebita a dare o promettere utilità
	art. 321	Pene per il corruttore
	art. 322	Istigazione alla corruzione
	art. 346	Traffico di influenze

5.2 Identificazione delle attività e delle operazioni a rischio

Le attività che MIT ha individuato come sensibili, nell'ambito della fattispecie di reato nei Rapporti con la Pubblica Amministrazione, sono indicate in dettaglio nella Matrice delle Attività a Rischio-Reato conservata a cura della Società, unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

Le attività individuate quali rilevanti per la SIM sono la gestione dei rapporti:

- di "alto profilo" con soggetti istituzionali e/o altri soggetti appartenenti a enti pubblici o incaricati di pubblici servizi per la promozione della SIM;
- con i funzionari della Guardia di Finanza, dell'Agenzia delle Entrate e degli altri enti competenti in materia fiscale, tributaria e societaria, anche in occasione di verifiche, ispezioni e accertamenti;
- con le Autorità di Vigilanza (Banca d'Italia, Consob, Borsa Italiana, Agenzia dell'Entrate, UIF ecc.), anche in occasione di verifiche, ispezioni ed accertamenti;

- con i funzionari degli enti competenti in materia di adempimenti societari presso il Tribunale, la CCIAA e l'Ufficio del Registro;
- con i Giudici, con i loro consulenti tecnici e con i loro ausiliari, nell'ambito di procedimenti giudiziari (civili, penali, amministrativi), con particolare riferimento alla nomina dei legali e dei consulenti tecnici e di parte;
- con i soggetti indagati o imputati in un procedimento penale;
- con i Giudici competenti, con i loro consulenti tecnici e con i loro ausiliari, nell'ambito delle cause di varia natura o dei relativi ricorsi.

Attraverso l'individuazione delle attività esposte al rischio di reato ("attività sensibili") e la strutturazione di un sistema di controllo interno volto alla prevenzione di tali rischi, MIT intende:

- da un lato, determinare una piena consapevolezza in tutti coloro che operano in nome e per conto di MIT di poter incorrere in un illecito passibile di sanzione e la cui commissione è fortemente censurata dalla SIM, in quanto sempre contraria ai suoi interessi anche quando, apparentemente, essa potrebbe trarne un vantaggio economico immediato;
- dall'altro, in virtù di un monitoraggio costante delle attività, consentire di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

5.3 Principi generali di comportamento

Coerentemente con i principi di cui alla Parte Generale del Modello Organizzativo ex D. Lgs. 231/2001 e del Codice Etico adottati dalla SIM, nello svolgimento delle attività sensibili sopra citate tutti i Destinatari del Modello sono tenuti ad osservare i principi di comportamento seguenti.

In linea generale, è fatto divieto ai Destinatari di influenzare le decisioni e l'indipendenza di giudizio dei Rappresentanti della Pubblica Amministrazione in maniera impropria e/o illecita.

In particolare, sono richieste:

- l'osservanza di tutte le leggi e i regolamenti che disciplinano la prestazione dei servizi di investimento e delle attività della SIM, con particolare riferimento alle attività che comportano rapporti con Enti pubblici, Pubbliche amministrazioni, Pubblici Ufficiali e Incaricati di Pubblici Servizi;
- l'instaurazione ed il mantenimento dei rapporti con la Pubblica Amministrazione secondo criteri di massima correttezza, trasparenza collaborazione e imparzialità.

Al fine di evitare il rischio di incorrere in reati contro la Pubblica Amministrazione:

- è fatto espresso divieto di effettuare, o acconsentire, ad elargizioni o promesse di denaro, beni o altre utilità di qualsiasi genere ad esponenti della Pubblica Amministrazione o a soggetti terzi da questi indicati o che abbiano con questi rapporti diretti o indiretti di qualsiasi natura, al fine di ottenere favori indebiti o benefici in violazione di norme di legge;
- è fatto espresso divieto di favorire consulenti/collaboratori/ fornitori, outsourcer o assegnare i relativi incarichi dietro specifica segnalazione dei Rappresentanti della Pubblica Amministrazione, in cambio di favori, compensi o altri vantaggi per sé e/o per la SIM;

- in particolare, non devono essere prese in esame eventuali segnalazioni provenienti da esponenti della Pubblica Amministrazione ai fini dell'assunzione presso la SIM di personale, o comunque dell'interessamento da parte della SIM alla assunzione o collocazione di questi presso terzi;
- non devono essere prese in esame segnalazioni provenienti dalla Pubblica Amministrazione relative all'indicazione di consulenti o partner, affinché la SIM li indichi a sua volta ai suoi consulenti o partner;
- non devono inoltre essere prese in considerazione richieste di sponsorizzazione, contributi elettorali, di trattamenti privilegiati provenienti da esponenti della Pubblica Amministrazione, in particolare se formulate in occasione di specifici affari od operazioni;
- è fatto espresso divieto di distribuire omaggi, regali, benefici non monetari o prestazione di qualsiasi natura al di fuori di quanto previsto dalle procedure aziendali – vale a dire, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore indebiti o non dovuti nella conduzione di qualsiasi attività aziendale. In particolare, è vietata qualsiasi forma di regalo a funzionari pubblici italiani ed esteri (anche in quei paesi in cui l'elargizione di doni rappresenta una prassi diffusa), a loro familiari o a soggetti da loro indicati, che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore;
- è fatto espresso divieto di scegliere collaboratori esterni per ragioni diverse da quelle connesse alla necessità, professionalità ed economicità e riconoscere ad essi compensi che non trovino adeguata giustificazione nel contesto del rapporto in essere e nel valore effettivo della prestazione.

5.4 Procedure di controllo

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito ulteriori presidi di controllo operativi a prevenzione della commissione dei reati in oggetto, con particolare riferimento ai principali processi strumentali a presidio delle aree in oggetto:

- gli incontri con la Pubblica Amministrazione sono gestiti e intrapresi solo da esponenti aziendali dotati di procura a rappresentare la società e possibilmente devono essere presenziati da due rappresentati aziendali;
- l'eventuale presenza nell'ambito dei membri del Consiglio d'Amministrazione di soggetti che abbiano anche incarichi o compiti pubblici deve esser preventivamente dichiarata, unitamente alla circostanza di aver successivamente assunto la qualifica di persona politicamente esposta, anche per l'espletamento di tutti gli adempimenti ai fini antiriciclaggio;
- degli incontri con la Pubblica Amministrazione deve essere tenuta traccia tramite informativa per iscritto corredata dell'eventuale documentazione richiesta e consegnata ai Soggetti Pubblici, trasmessa al responsabile e opportunamente archiviata (evidenziando ad es. data, obiettivi, motivazioni, partecipanti);
- gli incarichi conferiti a collaboratori esterni sono redatti per iscritto con l'indicazione del compenso pattuito e sono proposti, verificati e approvati da soggetti aziendali competenti nel rispetto del principio di separazione dei compiti;

- la liquidazione dei compensi ai consulenti, esterni è effettuata in modo trasparente, è documentata e sempre ricostruibile *ex post*;
- coloro che svolgono una funzione di controllo e supervisione su adempimenti connessi a richieste della Pubblica Amministrazione curano la corretta attuazione degli adempimenti e riferiscono immediatamente all'Organismo di Vigilanza eventuali situazioni di irregolarità.

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito l'elenco dei riferimenti normativi interni e delle procedure operative adottate dalla Società all'interno dei quali la Società ha definito i presidi di controllo a prevenzione della commissione dei reati in oggetto:

- Codice Etico;
- Procedura di selezione e di gestione dei fornitori e degli outsourcers;
- Procedura sulla gestione delle operazioni con parti correlate;
- Policy sulla gestione dei conflitti di interessi.

6. REATI SOCIETARI (ART. 25 ter)

6.1 Identificazione dei reati applicabili alla SIM

In conformità a quanto previsto all' art. 6, comma 2, lett. a) del D. Lgs. 231/2001 sono state identificate le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati inclusi nel Decreto.

Nello specifico, si elencano di seguito le fattispecie di reato contemplate nel D. Lgs. 231/2001 all' art. 25 *ter* ritenute applicabili, anche se in via prudenziale, a MIT, in ragione delle attività svolte, rimandando all'Allegato 1 della Parte Generale per l'elencazione completa dei reati inclusi nella presente famiglia di reato:

Art. D. Lgs. 231/2001	**REATI PRESUPPOSTO (Codice Penale)**	
25 ter– Reati Societari	art. 2621	False comunicazioni sociali
	art. 2622	False comunicazioni sociali in danno della società, dei soci o dei creditori
	art. 173 bis TUF	Falso in prospetto
	art. 2625	Impedito controllo
	art. 2626	Indebita restituzione dei conferimenti
	art. 2627	Illegale ripartizione degli utili e delle riserve
	art. 2628	Illecite operazioni sulle azioni o quote sociali o della società controllante
	art. 2629	Operazioni in pregiudizio dei creditori
	art. 2629-bis	Omessa comunicazione del conflitto di interessi
	art. 2632	Formazione fittizia del capitale
	art. 2365	Corruzione tra privati
	art. 2365 bis	Induzione alla corruzione tra privati
	art. 2636 c.c.	Illecita influenza sull'assemblea
	art. 2637 c.c.	Aggiotaggio
	art. 2638 c.c.	Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza

6.2 Identificazione delle attività e delle operazioni a rischio

Le attività che MIT ha individuato come sensibili, nell'ambito dei reati societari, sono indicate in dettaglio nella Matrice delle Attività a Rischio-Reato conservata a cura della SIM, unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

Le attività individuate quali rilevanti per la SIM sono:

- negoziazione in conto proprio (in contropartita diretta) e per conto terzi e relativa attività di *Specialist*, collocamento degli strumenti finanziari, trasmissione ed esecuzione degli ordini; funzione di Euronext Growth Advisor in sede di ammissione alla quotazione di società emittenti clienti della SIM ed eventuali connesse attività di Global Coordinator ed Euronext Growth Advisor per l'assistenza dopo l'ammissione alla quotazione da parte di detti emittenti;
- gestione delle attività operative di *trading, post trading* e controllo connesse alla prestazione dei servizi e delle attività di cui ai punti precedenti;
- gestione degli adempimenti operativi connessi agli abusi di mercato, per quanto applicabili;
- gestione della contabilità generale effettuata col supporto, per quanto di competenza, degli outsourcer incaricati;
- collaborazione e supporto al Consiglio d'Amministrazione per la predisposizione di situazioni patrimoniali funzionali alla realizzazione di operazioni straordinarie, operazioni di aumento/riduzione del capitale sociale, ripartizione degli utili d'esercizio, delle riserve e/o della restituzione dei conferimenti o altre operazioni su azioni o quote sociali o della società;
- raccolta, aggregazione e valutazione dei dati contabili necessari per la predisposizione, con il supporto degli *outsourcer* che si occupano delle registrazioni contabili e della predisposizione del bilancio d'esercizio o rendiconto annuale, delle relazioni semestrali e, ove redatti e resi pubblici, dei resoconti intermedi di gestione o le relazioni trimestrali, nonché delle relazioni allegate al Bilancio d'esercizio da sottoporre alla delibera del Consiglio di Amministrazione e dell'Assemblea dei Soci;
- gestione dei rapporti con gli Organi di Controllo relativamente alle verifiche sulla gestione amministrativa/contabile sul bilancio d'esercizio o rendiconto annuale, sulle relazioni semestrali e con i Soci nelle attività di verifica della gestione aziendale;
- tenuta delle scritture contabili e dei Libri Sociali, con il supporto dell'*outsourcer* che si occupa delle registrazioni contabili nonché con l'*outsourcer* che si occupa della tenuta, redazione ed aggiornamento dei Libri Sociali;
- collaborazione e supporto al Consiglio d'Amministrazione per l'effettuazione delle operazioni di incremento/riduzione del capitale sociale o di altre operazioni su azioni;
- gestione dei flussi monetari e finanziari;
- selezione, negoziazione, stipula ed esecuzione di contratti di acquisto di servizi, ivi compresi, a titolo esemplificativo, i contratti di esternalizzazione, riferita a soggetti privati, con particolare riferimento alla scelta della controparte. In particolare, ci si riferisce ad acquisti quali: consulenze direzionali, amministrativo-legali e collaborazioni a progetto; spese di rappresentanza; spese legate alla promozione della SIM, ai servizi amministrativi, ICT ecc.;
- predisposizione della documentazione che sarà oggetto di discussione e delibera in Assemblea e gestione dei rapporti con tale Organo Sociale;
- gestione dei rapporti e delle informazioni dirette alle Autorità di vigilanza e/o altre Autorità (es. Agenzia delle Entrate, UIF, REI, Anagrafe Tributaria, FATCA, CRS ecc.), anche in occasione di verifiche, ispezioni ed accertamenti.

Attraverso l'individuazione delle attività esposte al rischio di reato ("attività sensibili") e la strutturazione di un sistema di controllo interno volto alla prevenzione di tali rischi, MIT intende:

- da un lato, determinare una piena consapevolezza in tutti coloro che operano in nome e per conto di MIT di poter incorrere in un illecito passibile di sanzione e la cui commissione è fortemente censurata dalla SIM, in quanto sempre contraria ai suoi interessi anche quando, apparentemente, essa potrebbe trarne un vantaggio economico immediato;
- dall'altro, in virtù di un monitoraggio costante delle attività, consentire di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

6.3 Principi generali di comportamento

Coerentemente con i principi di cui alla Parte Generale del Modello Organizzativo ex D. Lgs. 231/2001 e del Codice Etico adottati dalla SIM, nello svolgimento delle attività sensibili sopra citate tutti i destinatari del Modello sono tenuti ad osservare i seguenti principi di comportamento:

- di agire, ciascuno secondo la propria funzione, in osservanza dei principi di correttezza, trasparenza e collaborazione, conformemente alle norme di legge, di regolamento, alle procedure aziendali esistenti, ai principi generalmente riconosciuti di tenuta della contabilità, in tutte le attività finalizzate alla redazione del bilancio d'esercizio o rendiconto annuale, delle relazioni semestrali e, ove redatti e resi pubblici, i resoconti intermedi di gestione oltre che le connesse comunicazioni sociali, al fine di fornire ai soci, ai terzi, alle istituzioni e al pubblico in genere un'informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della SIM;
- di agire, ciascuno secondo la propria funzione, in osservazione dei principi e norme di comportamento previste nella normativa applicabile per quanto attiene alla prestazione dei servizi ed attività di investimento cui la SIM è autorizzata, con particolare attenzione alle attività ed operazioni di *trading, post trading* e controllo delle medesime anche ai fini della materia del *market abuse*, per quanto applicabile;
- di agire, ciascuno secondo la propria funzione, in osservanza dei principi di correttezza, trasparenza e collaborazione, conformemente alle norme di legge, di regolamento e delle procedure aziendali esistenti, per quanto attiene alla definizione dei compensi variabili e alla loro effettiva distribuzione;
- di mantenere una condotta improntata ai principi di correttezza, trasparenza e collaborazione nell'acquisizione, elaborazione e comunicazione delle informazioni destinate a consentire agli azionisti e agli investitori di formarsi opinioni e/o giudizi sulla situazione patrimoniale, economica e finanziaria della SIM;
- di formalizzare delle linee guida che stabiliscano quali dati e notizie debbano essere forniti agli *outsourcer* che si occupano, tra l'altro, delle registrazioni contabili e della predisposizione del bilancio d'esercizio o rendiconto annuale, delle relazioni semestrali e, ove redatti e resi pubblici, i resoconti intermedi di gestione o le relazioni trimestrali, nonché quali controlli devono essere svolti dalla competente area amministrativa e coordinamento degli *outsourcer* interna alla SIM, sugli elementi forniti;

- di assicurare il regolare funzionamento della SIM e degli Organi Sociali, agevolando e garantendo ogni forma di controllo interno e promuovendo la libera formazione e assunzione delle decisioni collegiali;
- di stabilire in modo chiaro ed univoco la responsabilità dei diversi soggetti interni alla SIM oltre agli *outsourcer* coinvolti nella gestione dei dati contabili, garantendo la separazione delle funzioni e la coerenza dei livelli autorizzativi, nell'ambito della rilevazione, trasmissione e aggregazione delle informazioni contabili finalizzate alla predisposizione del bilancio d'esercizio o rendiconto annuale, delle relazioni semestrali e, ove redatti e resi pubblici, i resoconti intermedi di gestione oltre che le connesse comunicazioni sociali;
- di assicurare globalmente un adeguato presidio di controllo sulle registrazioni contabili routinarie e valutative, che devono essere svolte in modo accurato, corretto e veritiero, nonché rispettare i principi contabili di riferimento;
- di osservare le leggi in materia di tutela della concorrenza e del mercato e vigilare sulla perfetta osservanza delle stesse, nonché collaborare con le Autorità di Vigilanza per poter garantire la corretta trasparenza e pubblicità su tali aspetti, anche con riferimento ad eventuali tematiche connesse alla materia del *market abuse*, per quanto applicabile;
- di osservare i principi fondamentali quali l'onestà o l'integrità nel perseguimento del profitto della Società e di rispettare le leggi e le normative vigenti orientando le proprie azioni ed i propri comportamenti ai principi, agli obiettivi ed agli impegni richiamati nella normativa aziendale, con particolare riguardo al Codice Etico.

In particolare, è fatto espresso divieto ai soggetti interessati dai processi sensibili rilevati di:

- effettuare registrazioni contabili in modo non accurato, non corretto e non veritiero e/o fornire informazioni o documenti non veritieri agli *outsourcer* incaricati delle registrazioni contabili e della predisposizione del bilancio d'esercizio o rendiconto annuale, delle relazioni semestrali e, ove redatti e resi pubblici, dei resoconti intermedi di gestione o delle relazioni trimestrali;
- registrare operazioni senza un'adeguata documentazione di supporto che ne consenta *in primis* una corretta rilevazione contabile e successivamente una ricostruzione accurata;
- predisporre, rappresentare o trasmettere, per l'elaborazione del bilancio d'esercizio o del rendiconto annuale, delle relazioni semestrali e, ove redatti e resi pubblici, i resoconti intermedi di gestione o le relazioni trimestrali anni, dati falsi, lacunosi, incompleti o comunque suscettibili di fornire una descrizione non corretta della realtà ovvero omettere informazioni rilevanti in ordine alla situazione economica, patrimoniale e finanziaria della SIM;
- porre in essere o concorrere in qualsiasi forma nella realizzazione di comportamenti tali da integrare le fattispecie dei reati societari;
- porre in essere o concorrere in qualsiasi forma nella realizzazione di comportamenti che, sebbene risultino tali da non integrare un'ipotesi di reati societari, possono potenzialmente tradursi in tali illeciti o favorirne la commissione;
- alterare o, comunque, riportare in modo non corretto i dati e le informazioni destinati alla stesura di eventuali prospetti informativi;
- omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della SIM;

- omettere comunicazioni, da parte degli Amministratori, dall'Amministratore Delegato e Direttore Generale e/o degli altri Soggetti Rilevanti (come definiti nella Policy sulla gestione dei conflitti di interessi), di conflitti di interessi, tralasciando di precisarne natura, termini, origine e portata tali da poter inficiare le scelte del Consiglio di Amministrazione in merito ad operazioni di carattere ordinario e/o straordinario;
- restituire conferimenti ai soci o esentare i soci dall'effettuarli, al di fuori dei casi espressamente previsti dalla legge;
- ripartire utili (o acconti sugli utili) non effettivamente conseguiti o destinati per legge a riserva, nonché ripartire riserve (anche non costituite con utili) che non possano per legge essere distribuite;
- effettuare riduzioni del capitale sociale, fusioni o scissioni in violazione delle disposizioni di legge a tutela dei creditori;
- procedere in ogni modo a formazione o aumenti fittizi del capitale sociale;
- tenere comportamenti che impediscano materialmente, o che comunque ostacolino, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, lo svolgimento dell'attività di controllo o di revisione della gestione sociale da parte del Collegio Sindacale o della Società di Revisione;
- porre in essere, in occasione di assemblee, atti simulati e fraudolenti, finalizzati ad alterare il regolare procedimento di formazione della volontà assembleare;
- esporre nelle comunicazioni e nella documentazione trasmessa alle Autorità di Vigilanza fatti non rispondenti al vero o occultare fatti concernenti la situazione economica, patrimoniale e finanziaria della SIM;
- porre in essere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni da parte delle Autorità di Vigilanza, anche in sede di ispezioni (espressa opposizione, rifiuti pretestuosi, comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).

Al fine di prevenire il rischio che MIT possa essere imputata del reato di "Corruzione tra privati" /o di "Istigazione alla corruzione tra privati", è essenziale che ogni possibile relazione della Società con gli altri operatori privati, sia in sede di individuazione delle potenziali controparti contrattuali, di negoziazione di contratti sia di esecuzione degli stessi, anche nell'ambito della attività di Sales&Marketing, sia improntata a principi di correttezza e di trasparenza nonché a chiari principi di selezione.

E' fatto divieto ai Destinatari di influenzare le decisioni dei soggetti terzi alla SIM in maniera impropria e/o illecita. In particolare, è fatto loro divieto di:

- promettere o effettuare erogazioni in denaro, anche per interposta persona, a favore di soggetti terzi alla SIM per ottenere benefici in favore di MIT;
- promettere e/o offrire e/o corrispondere a soggetti terzi alla SIM, direttamente o tramite terzi, anche per interposta persona, somme di denaro o altre utilità in cambio di favori, compensi, sottoscrizione di azioni della SIM o altri vantaggi per MIT;
- effettuare pagamenti o riconoscere altre utilità, anche per interposta persona, a collaboratori, fornitori, consulenti, o altri soggetti terzi che operino per conto della SIM, che non trovino adeguata giustificazione nel rapporto contrattuale ovvero nella prassi vigente;
- favorire, anche per interposta persona, nei processi di acquisto di servizi, consulenti o altri soggetti dietro specifica segnalazione di soggetti terzi alla SIM, in cambio di favori, compensi o altri vantaggi per MIT;

- prendere in considerazione richieste di sponsorizzazione da parte di soggetti terzi che entrino in relazione con la SIM, se formulate in occasione di specifici affari od operazioni in cui è coinvolta tale controparte e la SIM;
- riconoscere e distribuire omaggi, regali, benefici non monetari o prestazione di qualsiasi natura al di fuori di quanto previsto dalle procedure aziendali - vale a dire, ogni forma di regalo offerto o ricevuto, eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore indebiti o non dovuti nella conduzione di qualsiasi attività aziendale;
- violare i diritti dei clienti sui beni affidati e la separazione patrimoniale tra i patrimoni dei singoli clienti e tra questi e il patrimonio della SIM;
- utilizzare, salvo consenso scritto dei clienti, gli strumenti finanziari o le disponibilità liquide di pertinenza dei clienti, detenuti a qualsiasi titolo.
- selezionare collaboratori esterni per ragioni diverse da quelle connesse alla necessità, professionalità ed economicità e riconoscere ad essi compensi che non trovino adeguata giustificazione nel contesto del rapporto in essere e nel valore effettivo della prestazione.

6.4 Procedure di controllo.

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito ulteriori presidi di controllo operativi a prevenzione della commissione dei reati in oggetto, con particolare riferimento ai principali processi strumentali a presidio delle aree in oggetto.

Flussi monetari e finanziari

- l'unità area amministrativa e coordinamento degli *outsourcer* unitamente all'Amministratore Delegato e Direttore Generale, col supporto dell'*outsourcer* incaricato della contabilità di bilancio e degli adempimenti fiscali ha la responsabilità, di verificare l'esistenza di autorizzazione alla spesa e qualora dovessero emergere dubbi sull'inerenza delle spese o sulla natura del servizio erogato, dovrà segnalarlo all'Amministratore Delegato e Direttore Generale e, ove necessario, anche alla Funzione Compliance, i quali dovranno effettuare adeguati approfondimenti e richiederne autorizzazione;
- l'impiego delle risorse finanziarie avviene mediante la definizione di soglie quantitative coerenti alle competenze gestionali e alle responsabilità organizzative affidate alle singole persone (procure a spendere);
- l'unità può disporre pagamenti solo a fronte di fatture registrate come pagabili nel sistema contabile o comunque preventivamente autorizzate dall'Amministratore Delegato e Direttore Generale;
- l'apertura/chiusura dei conti correnti deve essere preventivamente autorizzata dai soggetti dotati di idonei poteri;
- è vietata la concessione di rimborsi spese a soggetti diversi dagli Amministratori e dai Dipendenti della SIM, qualora non previsto dal contratto/lettera d'incarico (es.: consulenti/collaboratori); tali rimborsi sono liquidabili solo dietro presentazione di una fattura del soggetto stesso/società di riferimento o di idonea documentazione giustificativa riconosciuta come tale a termine di legge;

- non sono ammessi omaggi, regali e/o altri benefici non monetari che non si caratterizzino per l'esiguità del valore e che non siano allineati alle previsioni normative applicabili tempo per tempo;
- l'unità area amministrativa e coordinamento degli *outsourcer* unitamente all'Amministratore Delegato e Direttore Generale effettuano controlli periodici, di quadratura e riconciliazione dei dati contabili (es. riconciliazioni bancarie) con il supporto dell'*outsourcer* preposto;
- l'Amministratore Delegato e Direttore Generale elabora e gestisce la politica commerciale della Società avendo cura di definire il *pricing*, le condizioni di vendita, i rapporti con la clientela inclusi i termini di pagamento generali o particolari e concorre alla definizione del budget annuale per servizio, aggiornando le connesse rilevazioni andamentali alle scadenze prefissate;
- gli Uffici della SIM coinvolti per competenza, con il supporto degli *outsourcer* ai quali la SIM ha esternalizzato le principali attività amministrative e contabili, provvedono ad elaborare appositi report periodici finalizzati a monitorare, tra l'altro, l'andamento di business specifici, o di carattere più generale, nonché aventi anche natura previsionale;
- il Responsabile degli obblighi di salvaguardia dei beni dei clienti (che è anche Amministratore Delegato e Direttore Generale) nominato da parte della SIM è dotato di adeguate competenze e si occupa di salvaguardare gli strumenti finanziari e le disponibilità liquide dei clienti. Tale Responsabile è tenuto, in particolare, a (i) garantire i diritti dei clienti sui beni affidati e la separazione patrimoniale tra i patrimoni dei singoli clienti e tra questi e il patrimonio dell'intermediario finanziario; (ii) non consentire azioni dei creditori della SIM; (iii) non consentire, salvo espresso consenso del cliente, l'utilizzo nell'interesse proprio o di terzi, degli strumenti finanziari e delle disponibilità liquide di pertinenza dei clienti, detenuti a qualsiasi titolo.

Formazione del bilancio e rapporti con gli Organi di controllo

- le operazioni di rilevazione e registrazione delle attività devono essere effettuate con correttezza e nel rispetto del principio di veridicità, completezza e accuratezza;
- tutta la documentazione di supporto all'elaborazione del bilancio d'esercizio o rendiconto annuale, delle relazioni semestrali e, ove redatti e resi pubblici, dei resoconti intermedi di gestione o delle relazioni trimestrali è archiviata e conservata a cura;
- tutti i dati e le informazioni che servono alla redazione del bilancio d'esercizio o rendiconto annuale, delle relazioni semestrali e, ove redatti e resi pubblici, dei resoconti intermedi di gestione devono essere chiari, completi e rappresentare in modo veritiero la situazione economica, finanziaria e patrimoniale di MIT;
- i dati e le informazioni sono raccolti tempestivamente, sotto la supervisione dell'Amministratore Delegato e Direttore Generale ed elaborati da soggetti incaricati ai fini della predisposizione della bozza di bilancio. A richiesta, insieme ai dati e alle informazioni devono essere trasmessi anche gli eventuali documenti e le fonti da cui sono tratte le informazioni;
- è fatto divieto di porre in essere attività e/o operazioni volte a creare disponibilità extracontabili (ad esempio ricorrendo a rimborsi spese inesistenti o alla sovra fatturazione di consulenze), ovvero volte a creare "fondi neri" o "contabilità parallele". Una particolare attenzione deve essere dedicata alla stima delle poste contabili: i soggetti che intervengono nel procedimento di stima devono attenersi al rispetto del principio di ragionevolezza ed esporre con chiarezza i parametri di valutazione seguiti

nel rispetto dei principi contabili di riferimento, fornendo ogni informazione complementare che sia necessaria a garantire la veridicità e completezza del processo valutativo e di stima effettuato;

- la rilevazione, la trasmissione e l'aggregazione dei dati e delle informazioni contabili, per la redazione del bilancio di esercizio, devono avvenire con modalità tali da assicurare che vi sia sempre evidenza dei passaggi del processo di formazione dei dati, e sia sempre individuabile il soggetto che ha effettuato la richiesta di inserimento dati, inserito i dati nel sistema contabile, approvato i dati contabili risultanti;
- l'Amministratore Delegato e Direttore Generale, incaricato della raccolta ed elaborazione delle informazioni richieste e trasmesse al Collegio Sindacale, deve garantire la completezza, inerenza e correttezza della documentazione trasmessa;
- la calendarizzazione delle attività di chiusura e la relativa comunicazione da parte dell'Amministratore Delegato e Direttore Generale avviene in forma scritta a tutti i soggetti interessati;
- sono svolte attività di analisi del bilancio di verifica, predisposizione dei prospetti di bilancio ed evidenza della condivisione con il management, condivisione con gli organi di controllo e approvazione del bilancio d'esercizio;
- è mantenuta evidenza scritta e tracciabilità della consegna della bozza di bilancio a tutti i componenti del Consiglio di Amministrazione, prima della riunione per approvazione dello stesso, nei tempi di legge previsti;
- è mantenuta evidenza scritta e tracciabilità della consegna dell'attestazione di bilancio da parte della Società di revisione e siglata dall'Amministratore Delegato e Direttore Generale;
- è mantenuta evidenza scritta e tracciabilità degli incontri periodici (almeno annuale) tra la Società di revisione, Organismo di Vigilanza e Consiglio Sindacale prima dell'approvazione del bilancio d'esercizio o rendiconto annuale, delle relazioni semestrali e, ove redatti e resi pubblici, dei resoconti intermedi di gestione da parte del Consiglio di Amministrazione;
- eventuali conflitti di interessi da parte degli Amministratori, precisandone natura, termini, origine e portata, sono tempestivamente comunicati al Consiglio di Amministrazione e al Collegio Sindacale se rientrano tra quelli sopra soglia di rilevanza previsti nell'apposita Policy sulla gestione dei conflitti di interessi e nelle apposite procedure interne in materia;
- i comunicati stampa sono verificati dall'Amministratore Delegato e Direttore Generale, prima della diffusione al mercato;
- è garantita tracciabilità del processo decisionale di acquisti e vendite di azioni proprie, unitamente alla definizione dei piani industriali a supporto delle stesse.

Acquisti di servizi e consulenze

- è necessario tutelare la separazione dei compiti tra chi approva la consulenza e chi approva il pagamento della prestazione;
- al fine di garantire criteri di concorrenza, economicità, trasparenza, correttezza e professionalità, l'identificazione del fornitore di servizi e consulenze dovrà avvenire

mediante valutazione comparativa di più offerte secondo i criteri previsti dalle procedure aziendali e/o la verifica che la consulenza sia fornita a valori di mercato;

- la scelta del fornitore di servizi o consulenti è fondata su criteri di valutazione oggettivi requisiti di professionalità ed onorabilità quali a titolo esemplificativo e non esaustivo: presenza e verifica dei requisiti di professionalità, comprovata esperienza nel settore ed onorabilità, condizioni praticate, affidamento di precedenti forniture, iscrizione ad albi professionali);
- l'acquisto di servizi e consulenze deve essere documentato in un contratto/lettera di incarico formalmente approvato da soggetti dotati di idonei poteri.

I contratti di acquisto e le lettere di incarico con i professionisti/consulenti, i fornitori e gli *outsourcer* devono contenere l'informativa sulle norme comportamentali adottate dalla SIM relativamente al Modello Organizzativo e al relativo Codice Etico (per la cui consultazione si rinvierà al sito internet della SIM), nonché sulle conseguenze che comportamenti contrari alle previsioni del Codice Etico, ai principi comportamentali che ispirano MIT e alle normative vigenti, possono avere con riguardo ai rapporti contrattuali. In particolare, nell'ambito di tali previsioni contrattuali è inoltre previsto che, la violazione delle procedure, dei modelli comportamentali e delle prescrizioni contenuti nel Modello Organizzativo ex D.Lgs. 231/2001 e/o nel Codice Etico possono comportare, in caso di ragionevole e motivata necessità, l'immediata risoluzione del rapporto contrattuale per fatto e colpa della controparte. In tal caso, quest'ultima è tenuta a risarcire e tenere indenne la SIM per le perdite, i danni, le spese, le responsabilità e le azioni che possano derivare dalla predetta violazione.

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito l'elenco dei riferimenti normativi interni e delle procedure operative adottate dalla Società all'interno dei quali la Società ha definito i presidi di controllo a prevenzione della commissione dei reati in oggetto:

- Codice Etico;
- Policy sui conflitti di interesse;
- Procedura sulla gestione delle operazioni con parti correlate;
- Procedura selezione e gestione dei fornitori e *outsourcer*;
- Procedura relativa alla gestione e diffusione di informazioni privilegiate e di operazioni sul capitale;
- Procedura sulla tenuta del registro insider;
- Procedura *Internal Dealing;*
- Procedura di gestione delle operazioni personali;
- Regolamento del Consiglio d'Amministrazione;
- Nomina del Responsabile degli obblighi di salvaguardia dei beni dei clienti;
- Tutte le procedure aziendali (con particolare riferimento alla fattispecie di reato di Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza).

7. DELITTI CON FINALITA' DI TERRORISMO (ART. 25 quater)

7.1 Identificazione dei reati applicabili alla SIM

In conformità a quanto previsto all' art. 6, comma 2, lett. a) del D. Lgs. 231/2001 sono state identificate le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati inclusi nel Decreto.

Nello specifico, si elencano di seguito le fattispecie di reato contemplate nel D. Lgs. 231/2001 all' art. 25 quater ritenute applicabili, anche se in via prudenziale, a MIT, in ragione delle attività svolte, rimandando all'Allegato 1 della Parte Generale per l'elencazione completa dei reati inclusi nella presente famiglia di reato:

Art. D. Lgs. 231/2001	**REATI PRESUPPOSTO (Codice Penale)**	
25 quater – Delitti con finalità di terrorismo	art. 270 bis c.p.	Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico
	art. 270 ter c.p.	Assistenza agli associati
	art. 270 quater c.p.	Arruolamento con finalità di terrorismo anche internazionale
	art. 270 quinquies c.p.	Addestramento ad attività con finalità di terrorismo anche internazionale
	art. 270 sexies c.p.	Condotte con finalità di terrorismo
	art. 280 c.p.	Attentato per finalità terroristiche o di eversione
	art. 280 bis c.p.	Atto di terrorismo con ordigni micidiali o esplosivi
	art. 289 bis c.p.	Sequestro di persona a scopo di terrorismo o di eversione
	art. 1 D.lg. 15/12/1979, n. 625 conv. con mod. in l. 6/02/1980, n. 15	Misure urgenti per la tutela dell'ordine democratico e della sicurezza pubblica
	art. 2	Convenzione internazionale per la repressione del finanziamento del terrorismo New York 9 dicembre 1999

7.2 Identificazione delle attività e delle operazioni a rischio

Le attività che MIT ha individuato come sensibili, nell'ambito dei delitti con finalità di terrorismo, sono indicate in dettaglio nella Matrice delle Attività a Rischio-Reato conservata a cura della Società, unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

Le attività individuate quali rilevanti per la SIM sono:

- prestazione dei servizi di investimento autorizzati (ricezione, trasmissione ed esecuzione degli ordini della clientela, negoziazione in conto proprio anche in contropartita diretta nei confronti dei clienti, collocamento senza assunzione di impegno irrevocabile nei confronti dell'emittente), con modalità operativa della detenzione, anche in via temporanea, delle disponibilità liquide e degli strumenti finanziari della clientela;
- il ruolo di *Euronext Growth Advisor* - EGA in sede di ammissione alla quotazione delle società emittenti o nell'ambito delle attività connesse a quelle di Global Coordinator ed EGA per l'assistenza post ammissione alla quotazione degli emittenti;
- lo svolgimento delle attività di *specialist* a supporto degli Emittenti di strumenti finanziari ammessi alla negoziazione sul mercato *Euronext Growth Milan* (EGM) o di *liquidity provider* su altri mercati borsistici;
- la selezione e la gestione dei fornitori e degli *outsourcer* e dei relativi processi.

Attraverso l'individuazione delle attività esposte al rischio di reato ("attività sensibili") e la strutturazione di un sistema di controllo volto alla prevenzione di tali rischi, MIT intende:

- da un lato, determinare una piena consapevolezza in tutti coloro che operano in nome e per conto di MIT di poter incorrere in un illecito passibile di sanzione e la cui commissione è fortemente censurata dalla SIM, in quanto sempre contraria ai suoi interessi anche quando, apparentemente, essa potrebbe trarne un vantaggio economico immediato;
- dall'altro, in virtù di un monitoraggio costante delle attività, consentire di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

7.3 Principi generali di comportamento

Coerentemente con i principi di cui alla Parte Generale del Modello Organizzativo ex D.Lgs.231/2001 e del Codice Etico adottati dalla SIM, nello svolgimento delle attività sensibili sopra citate tutti i Destinatari del Modello sono tenuti ad osservare i principi di comportamento seguenti:

- divieto di concludere operazioni con o in favore di soggetti (consulenti, fornitori, *outsourcer*, clienti ecc.) i cui nominativi siano contenuti nelle Liste antiterrorismo.

7.4 Procedure di controllo

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito l'elenco dei riferimenti normativi interni e delle procedure operative adottate dalla Società all'interno dei quali la Società ha definito i presidi di controllo a prevenzione della commissione dei reati in oggetto:

- Codice Etico;
- Policy e Procedura AML;
- Metodologia di valutazione dei rischi di riciclaggio;
- Politica di trasmissione e di esecuzione degli ordini della clientela;

- Procedura Servizio di negoziazione in conto proprio – Operatore specialista;
- Procedura relativa al collocamento degli strumenti finanziari;
- Procedura in materia di selezione e gestione dei fornitori ed *outsourcers.*

8. ABUSO DI INFORMAZIONI PRIVILEGIATE (ART. 25 sexies)

8.1 Identificazione dei reati applicabili alla SIM

In conformità a quanto previsto all' art. 6, comma 2, lett. a) del D. Lgs. 231/2001 sono state identificate le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati inclusi nel Decreto.

Nello specifico, si elencano di seguito le fattispecie di reato contemplate nel D. Lgs. 231/2001 all' art. 25 sexies ritenute applicabili, anche se in via prudenziale, a MIT, in ragione delle attività svolte, rimandando all'Allegato 1 della Parte Generale per l'elencazione completa dei reati inclusi nella presente famiglia di reato:

Art. D. Lgs. 231/2001	**REATI PRESUPPOSTO (Codice Penale)**	
25 sexties – Abuso di informazioni privilegiate	art. 184	Abuso di informazioni privilegiate
	art. 185	Manipolazione di mercato

8.2 Identificazione delle attività e delle operazioni a rischio

Le attività che MIT ha individuato come sensibili, nell'ambito dell'abuso di informazioni privilegiate, sono indicate in dettaglio nella Matrice delle Attività a Rischio-Reato conservata a cura della Società, unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

Le attività individuate quali rilevanti per la SIM sono:

- trattamento delle informazioni privilegiate e della relativa operatività in strumenti finanziari;
- predisposizione dei comunicati stampa e comunicazioni al mercato ed eventuali ritardi nella pubblicazione dei comunicati stampa;
- operazioni di *internal dealing*;
- operazioni personali.

Attraverso l'individuazione delle attività esposte al rischio di reato ("attività sensibili") e la strutturazione di un sistema di controllo interno volto alla prevenzione di tali rischi, MIT intende:

- da un lato, determinare una piena consapevolezza in tutti coloro che operano in nome e per conto di MIT di poter incorrere in un illecito passibile di sanzione e la cui commissione è fortemente censurata dalla SIM, in quanto sempre contraria ai suoi interessi anche quando, apparentemente, essa potrebbe trarne un vantaggio economico immediato;
- dall'altro, in virtù di un monitoraggio costante delle attività, consentire di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

8.3 Principi generali di comportamento

Coerentemente con i principi di cui alla Parte Generale del Modello Organizzativo ex D. Lgs. 231/2001 e del Codice Etico adottati dalla SIM, nello svolgimento delle attività sensibili sopra citate tutti i Destinatari del Modello sono tenuti ad osservare i principi di comportamento seguenti.

È fatto espresso obbligo ai Destinatari di trattare con la massima riservatezza tutte le informazioni privilegiate di cui dovessero venire a conoscenza nell'esercizio delle proprie funzioni, al fine sia di tutelare l'interesse della SIM al riserbo sui propri affari, sia di evitare abusi di mercato.

In ogni caso è fatto divieto ai Soggetti Interessati:

- di utilizzare informazioni privilegiate al fine di acquisire o cedere gli strumenti finanziari cui tali informazioni si riferiscono, per conto proprio o di terzi, direttamente o indirettamente o divulgandole a terzi, sia prima della loro diffusione ai sensi della procedura per il trattamento delle informazioni privilegiate sia secondo le disposizioni di legge e regolamentari applicabili, nonché in base a quanto espressamente previsto nella procedura della Società in materia di *internal dealing*;
- di utilizzare informazioni privilegiate, annullando o modificando un ordine concernente uno strumento finanziario al quale le informazioni si riferiscono, qualora tale ordine sia stato inoltrato prima che lo stesso Soggetto Rilevante entrasse in possesso di dette informazioni privilegiate;
- di raccomandare, divulgare ad altri o indurre altri, sulla base delle informazioni privilegiate in proprio possesso, ad effettuare operazioni sugli strumenti finanziari cui tali informazioni privilegiate si riferiscono.

8.4 Procedure di controllo

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito ulteriori presidi di controllo operativi a prevenzione della commissione dei reati in oggetto, con particolare riferimento ai principali processi strumentali a presidio delle aree in oggetto:

- tutti i dipendenti, i collaboratori ed i consulenti terzi che entrano in contatto con la SIM sono tenuti alla stretta osservanza delle previsioni normative in materia di trattamento delle informazioni privilegiate e di abusi di mercato;
- ai sensi dell'art. 18 del Regolamento (UE) 596/2014 e del Regolamento di Esecuzione 2016/347, la SIM ha istituito e aggiorna regolarmente l'Elenco delle persone che hanno accesso ad informazioni privilegiate (il Registro) di tutti coloro che, su base regolare od occasionale, hanno accesso a informazioni privilegiate e di tutti i soggetti con cui la SIM o le persone che agiscono a nome o per conto della stessa o abbiano un rapporto di collaborazione professionale e che, nello svolgimento di determinati compiti, hanno accesso a informazioni privilegiate (quali ad esempio consulenti, contabili, collaboratori esterni etc.);
- ai sensi di quanto previsto dalla Linee Guida Consob del 13 ottobre 2017 denominate *Gestione delle informazioni privilegiate*, la SIM ha istituito la Funzione Interna Gestione

delle Informazioni Privilegiate – FIGIP e ha affidato i relativi compiti all'Amministratore Delegato e Direttore Generale;

- i Destinatari pongono in essere ogni misura e cautela atta a:
  - evitare l'accesso e la circolazione di informazioni riservate che possano avere natura di informazioni privilegiate a persone non autorizzate, mantenendo riservati tutti i documenti e le informazioni acquisite nello svolgimento dei propri compiti;
  - mantenere segregate le informazioni che abbiano natura di informazioni privilegiate affinché l'accesso alle medesime avvenga soltanto da parte di chi è autorizzato sino a che dette informazioni non siano rese pubbliche, in applicazione delle disposizioni tempo per tempo vigenti in materia di pubblicazione delle informazioni privilegiate o ritardo nella pubblicazione nei casi previsti;
  - utilizzare i suddetti documenti e le suddette informazioni esclusivamente nell'espletamento delle loro funzioni;
  - assicurare che l'apertura e la distribuzione della corrispondenza pervenuta tramite il servizio postale e/o posta elettronica sia operata nel rispetto dei criteri di riservatezza;
- i Destinatari che dispongano di documenti o informazioni riservati devono custodirli in modo da ridurre al minimo, mediante l'adozione di idonee misure di sicurezza, i rischi di accesso e di trattamento non autorizzato;
- il mittente di documenti cartacei e/o elettronici aventi ad oggetto informazioni privilegiate deve evidenziarne il carattere strettamente riservato apponendo la dicitura "STRETTAMENTE RISERVATO";
- in caso di smarrimento di documenti relativi a informazioni privilegiate, i Destinatari coinvolti ne informano senza indugio la FIGIP, specificandone condizioni e circostanze, affinché questi possa adottare gli opportuni provvedimenti, ivi inclusa la pubblicazione di un comunicato;
- è fatto divieto ai Destinatari di comunicare all'esterno informazioni privilegiate prima della loro diffusione al mercato e delle disposizioni di legge e regolamentari applicabili.

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito l'elenco dei riferimenti normativi interni e delle procedure operative adottate dalla Società all'interno dei quali la Società ha definito i presidi di controllo a prevenzione della commissione dei reati in oggetto:

- Codice Etico;
- Procedura relativa alla gestione e diffusione di informazioni privilegiate e di operazione sul capitale;
- Procedura sulla tenuta del registro insider;
- Procedura *Internal Dealing*;
- Procedura di gestione delle operazioni personali.

9. REATI IN TEMA DI TUTELA DELLA SALUTE E SICUREZZA NEI LUOGHI DI LAVORO (ART. 25 septies)

9.1 Identificazione dei reati applicabili alla SIM

In conformità a quanto previsto all' art. 6, comma 2, lett. a) del D. Lgs. 231/2001 sono state identificate le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati inclusi nel Decreto.

Nello specifico, si elencano di seguito le fattispecie di reato contemplate nel D. Lgs. 231/2001 all' art. 25 septies ritenute applicabili, anche se in via prudenziale, a MIT, in ragione delle attività svolte, rimandando all'Allegato 1 della Parte Generale per l'elencazione completa dei reati inclusi nella presente famiglia di reato:

Art. D. Lgs. 231/2001	**REATI PRESUPPOSTO (Codice Penale)**	
25 septies – Reati in tema di tutela della salute e sicurezza sul luogo di lavoro	art. 589	Omicidio colposo
	art. 590	Lesioni personali colpose

9.2 Identificazione delle attività e delle operazioni a rischio

Le attività che MIT ha individuato come sensibili, nell'ambito della tutela della salute e sicurezza nei luoghi di lavoro, sono indicate in dettaglio nella Matrice delle Attività a Rischio-Reato conservata a cura della Società, unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

Le attività individuate quali rilevanti per la SIM sono:

- gestione del personale;
- gestione della salute e sicurezza;
- gestione immobili e logistica.

Attraverso l'individuazione delle attività esposte al rischio di reato ("attività sensibili") e la strutturazione di un sistema di controllo interno volto alla prevenzione di tali rischi, MIT intende:

- da un lato, determinare una piena consapevolezza in tutti coloro che operano in nome e per conto di MIT di poter incorrere in un illecito passibile di sanzione e la cui commissione è fortemente censurata dalla SIM, in quanto sempre contraria ai suoi interessi anche quando, apparentemente, essa potrebbe trarne un vantaggio economico immediato;
- dall'altro, in virtù di un monitoraggio costante delle attività, consentire di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

9.3 Principi generali di comportamento

Coerentemente con i principi di cui alla Parte Generale del Modello Organizzativo ex D.Lgs. 231/2001 e del Codice Etico adottati dalla SIM, nello svolgimento delle attività sensibili sopra citate tutti i Destinatari del Modello sono tenuti ad osservare i principi di comportamento seguenti:

- rispetto delle norme antinfortunistiche;
- rispetto delle norme igienico sanitarie Covid-19;
- rispetto della normativa in materia di salute e sicurezza sui luoghi di lavoro.

9.4 Procedure di controllo

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito l'elenco dei riferimenti normativi interni e delle procedure operative adottate dalla Società all'interno dei quali la Società ha definito i presidi di controllo a prevenzione della commissione dei reati in oggetto:

- Codice Etico;
- adempimenti obblighi normativi ex. D. Lgs. 81/2008:
    - corsi di formazione;
    - mappatura rischi a cui sono sottoposti gli addetti;
    - piano gestione emergenze;
    - verifiche periodiche da parte del RSPP;
    - presenza DPI;
    - attuazione della sorveglianza sanitaria dei lavoratori ed eventuale allontanamento degli stessi dall'esposizione al rischio a tutela della loro incolumità;
    - adozione di adeguate misure di primo soccorso, di prevenzione degli incendi e di lotta antincendio, di evacuazione dei luoghi di lavoro in caso di pericolo grave e immediato e, più in generale, di gestione delle emergenze, designando preventivamente i lavoratori incaricati della loro attuazione;
    - adozione di strumentazione e attrezzature di lavoro con omologazione CE;
- policy di controllo diffusione Coronavirus;
- procedura Green Pass*, pro tempore* vigente;
- monitoraggio continuativo della conformità agli obblighi di legge e delle normative aziendali, attraverso la programmazione ed effettuazione di verifiche interne su sicurezza ed ambiente opportunamente diffuse e documentate (con indicazione di: eventuali criticità emerse, azioni da intraprendere, tempi di attuazione e responsabili della loro attuazione).

10. REATI DI RICETTAZIONE, RICICLAGGIO E IMPIEGO DENARO, BENI O UTILITÀ, AUTORICICLAGGIO (ART. 25 octies)

10.1 Identificazione dei reati applicabili alla SIM

In conformità a quanto previsto all' art. 6, comma 2, lett. a) del D. Lgs. 231/2001 sono state identificate le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati inclusi nel Decreto.

Nello specifico, si elencano di seguito le fattispecie di reato contemplate nel D. Lgs. 231/2001 all' art. 25 octies ritenute applicabili, anche se in via prudenziale, a MIT, in ragione delle attività svolte, rimandando all'Allegato 1 della Parte Generale per l'elencazione completa dei reati inclusi nella presente famiglia di reato:

Art. D. Lgs. 231/2001	**REATI PRESUPPOSTO (Codice Penale)**	
25 octies – Reati di ricettazione, riciclaggio e impiego denaro, beni o utilità, autoriciclaggio	art. 648 bis	Riciclaggio
	art. 648 ter	Impiego di denaro, beni o utilità di provenienza illecita
	art. 648 ter 1	Autoriciclaggio

10.2 Identificazione delle attività e delle operazioni a rischio

Le attività che MIT ha individuato come sensibili, nell'ambito del Riciclaggio, sono indicate in dettaglio nella Matrice delle Attività a Rischio-Reato conservata a cura della Società, unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

Le attività individuate quali rilevanti per la SIM sono la gestione:

- prestazione dei servizi di investimento autorizzati (ricezione, trasmissione ed esecuzione degli ordini della clientela, negoziazione in conto proprio anche in contropartita diretta nei confronti dei clienti, collocamento senza assunzione di impegno irrevocabile nei confronti dell'emittente), con modalità operativa della detenzione, anche in via temporanea, delle disponibilità liquide e degli strumenti finanziari della clientela;
- il ruolo di *Euronext Growth Advisor* - EGA in sede di ammissione alla quotazione delle società emittenti o nell'ambito delle attività connesse a quelle di Global Coordinator ed EGA per l'assistenza post ammissione alla quotazione degli emittenti;
- lo svolgimento delle attività di *specialist* a supporto degli Emittenti di strumenti finanziari ammessi alla negoziazione sul mercato *Euronext Growth Milan* (EGM) o di *liquidity provider* su altri mercati borsistici;
- la selezione e la gestione dei fornitori e degli *outsourcer* e dei relativi processi;
- gestione degli adempimenti fiscali e tributari.

Attraverso l'individuazione delle attività esposte al rischio di reato ("attività sensibili") e la strutturazione di un sistema di controllo interno volto alla prevenzione di tali rischi, MIT intende:

- da un lato, determinare una piena consapevolezza in tutti coloro che operano in nome e per conto di MIT di poter incorrere in un illecito passibile di sanzione e la cui commissione è fortemente censurata dalla SIM, in quanto sempre contraria ai suoi interessi anche quando, apparentemente, essa potrebbe trarne un vantaggio economico immediato;
- dall'altro, in virtù di un monitoraggio costante delle attività, consentire di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

10.3 Principi generali di comportamento

Coerentemente con i principi di cui alla Parte Generale del Modello Organizzativo ex D.Lgs. 231/2001 e del Codice Etico adottati dalla SIM, nello svolgimento delle attività sensibili sopra citate tutti i Destinatari del Modello sono tenuti ad osservare i principi di comportamento seguenti:

- obbligo di approfondita conoscenza della clientela e delle controparti e di osservanza degli adempimenti previsti dalla articolata normativa aziendale in tema di contrasto al riciclaggio dei proventi di attività criminose ed al finanziamento del terrorismo;
- obbligo di identificazione e di adeguata verifica anche rafforzata, profilatura e monitoraggio del rischio su base continuativa;
- obbligo di rispettare rigorosamente le procedure interne in tema di registrazione dei rapporti e delle operazioni in AUI e di conservazione della documentazione;
- obbligo di segnalazione di operazioni sospette;
- obbligo di collaborazione attiva nei confronti delle Autorità di Vigilanza ai fini del contrasto al riciclaggio dei proventi di attività criminose ed al finanziamento del terrorismo.

10.4 Procedure di controllo

Le principali regole comportamentali di carattere generale sopraindicate sono dettagliate nella Policy e nelle procedure operative adottate dalla Società all'interno delle quali sono definite le responsabilità in materia i presidi di controllo a prevenzione della commissione dei reati in oggetto:

- Codice Etico;
- Policy e Procedura AML;
- Metodologia di valutazione del rischio di riciclaggio;
- Politica di trasmissione e di esecuzione degli ordini della clientela;
- Procedura "Servizio di negoziazione in conto proprio – Operatore specialista;
- Procedura relativa al collocamento degli strumenti finanziari;
- Procedura in materia di selezione e gestione dei fornitori ed *outsourcers*.

11. DELITTI IN MATERIA DI VIOLAZIONE DEI DIRITTI D'AUTORE (ART. 25 novies)

11.1 Identificazione dei reati applicabili alla SIM

In conformità a quanto previsto all' art. 6, comma 2, lett. a) del D. Lgs. 231/2001 sono state identificate le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati inclusi nel Decreto.

Nello specifico, si elencano di seguito le fattispecie di reato contemplate nel D. Lgs. 231/2001 all' art. 25 novies ritenute applicabili, anche se in via prudenziale, a MIT, in ragione delle attività svolte, rimandando all'Allegato 1 della Parte Generale per l'elencazione completa dei reati inclusi nella presente famiglia di reato:

Art. D. Lgs. 231/2001	**REATI PRESUPPOSTO (Codice Penale)**	
25 novies – Delitti in materia di violazione del diritto d'autore	art. 171, 171 bis, 171 septies 171 octies	Violazioni nei confronti della SIAE

11.2 Identificazione delle attività e delle operazioni a rischio

Le attività che MIT ha individuato come sensibili, nell'ambito di violazione dei diritti d'autore, sono indicate in dettaglio nella matrice delle attività a Rischio-Reato conservata a cura della Società, unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

Le attività individuate quali rilevanti per la SIM sono:

- selezione e gestione dei fornitori e degli outsourcer.

Alla luce dei presupposti applicativi della fattispecie in esame, la SIM potrebbe essere considerata responsabile per i delitti commessi nel suo interesse o vantaggio da persone che rivestono funzioni di amministrazione, rappresentanza, ma anche da persone sottoposte alla loro direzione o vigilanza che svolgono attività esternalizzate.

Le tipologie di reato di violazione del diritto d'autore si riferiscono, ad esempio, alla eventuale duplicazione, per trarne profitto, di programmi per elaboratore o l'importazione o detenzione a scopo commerciale o imprenditoriale di questi, per le medesime finalità.

In particolare, come già illustrato, nell'ambito dei sistemi informativi e contabili della SIM ve ne sono diversi che sono infatti utilizzati nell'ambito della prestazione dei servizi ed attività di investimento a cui è autorizzata. Si tratta, in particolare:

- di una apposita piattaforma fornita da un provider esterno che ha come finalità quella di consentire alla SIM di poter svolgere tutte le attività di *trading, post trading* e di controllo delle attività di *specialist* e per quelle relative alla prestazione dei servizi di investimento, che dialoga con le soluzioni informative che sono fornite dall'*outsourcer* a cui è affidato lo svolgimento delle attività amministrative e contabili;

- piattaforma per la postazione di trading (Bloomberg);
- di un applicativo per analizzare l'operatività ed individuare e segnalare alla competente Autorità di Vigilanza eventuali operazioni sospette ai fini del *market abuse*;
- di un applicativo per poter accedere alla consultazione della contabilità societaria e di prodotto ed ai dati relativi alle attività amministrative (*back office*) per la produzione delle segnalazioni nei confronti delle competenti Autorità di Vigilanza.

Inoltre, talune condotte criminose che, in via del tutto residuale, potrebbero manifestarsi sono quelle in occasione di eventi istituzionali, convegni, eventi o sponsorizzazioni nonché nell'ambito dell'utilizzo dei sistemi di segreteria telefonica e di risponditori automatici nel caso in cui non venissero pagati, ove necessario, i relativi diritti d'autore connessi ai materiali audio e video utilizzati.

Attraverso l'individuazione delle attività esposte al rischio di reato ("attività sensibili") e la strutturazione di un sistema di controllo interno volto alla prevenzione di tali rischi, MIT intende:

- da un lato, determinare una piena consapevolezza in tutti coloro che operano in nome e per conto di MIT di poter incorrere in un illecito passibile di sanzione e la cui commissione è fortemente censurata dalla SIM, in quanto sempre contraria ai suoi interessi anche quando, apparentemente, essa potrebbe trarne un vantaggio economico immediato;
- dall'altro, in virtù di un monitoraggio costante delle attività, consentire di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

11.3 Principi generali di comportamento

Coerentemente con i principi di cui alla Parte Generale del Modello Organizzativo ex D.Lgs.231/2001 e del Codice Etico adottati dalla SIM, nello svolgimento delle attività sensibili sopra citate tutti i Destinatari del Modello sono tenuti ad osservare i principi di comportamento seguenti:

- adozione di regole comportamentali che vietano comportamenti atti a ledere diritti di proprietà intellettuale altrui, assicurando il rispetto delle leggi e delle disposizioni regolamentari nazionali, comunitarie e internazionali poste a tutela della proprietà industriale, intellettuale e del diritto d'autore;
- la Società garantisce che i software di terzi utilizzati per lo svolgimento delle attività aziendali, siano opportunamente identificati e che il pagamento delle licenze ai rispettivi fornitori sia oggetto di un controllo periodico, garantendo nel tempo il monitoraggio della numerosità e le "generalità" degli applicativi di terzi;
- adozione di una regola comportamentale in forza della quale viene richiesto ai dipendenti di curare diligentemente gli adempimenti di carattere amministrativo connessi all'utilizzo di opere protette dal diritto d'autore (software, banche dati, ecc.) nell'ambito dell'utilizzo di applicazioni software di terzi;
- per quanto attiene all'uso delle dotazioni informatiche, è richiesto ai dipendenti di non:
    - utilizzare in azienda apparecchiature informatiche private, connettendole in qualsiasi modo alla rete informatica aziendale;

- installare sui computer o sui dispositivi aziendali assegnati programmi (software) provenienti dall'esterno ovvero dispositivi di memorizzazione, comunicazione o altro (modem, chiavi USB);
- copiare su un qualunque supporto multimediale atto a contenere dati di qualsiasi natura protetti dalla normativa a tutela del diritto d'autore.

11.4 Procedure di controllo

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito l'elenco dei riferimenti normativi interni e delle procedure operative adottate da parte di MIT all'interno dei quali essa ha definito i presidi di controllo a prevenzione della commissione dei reati in oggetto:

- Codice Etico;
- Procedura di selezione e gestione dei fornitori e degli *outsourcers.*

12. INDUZIONE A NON RENDERE DICHIARAZIONI MENDACI (ART. 25 decies)

12.1 Identificazione dei reati applicabili alla SIM

In conformità a quanto previsto all' art. 6, comma 2, lett. a) del D. Lgs. 231/2001 sono state identificate le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati inclusi nel Decreto.

Nello specifico, si elencano di seguito le fattispecie di reato contemplate nel D. Lgs. 231/2001 all' art. 25 decies ritenute applicabili, anche se in via prudenziale, a MIT, in ragione delle attività svolte, rimandando all'Allegato 1 della Parte Generale per l'elencazione completa dei reati inclusi nella presente famiglia di reato:

Art. D. Lgs. 231/2001	**REATI PRESUPPOSTO (Codice Penale)**	
Art. 25 decies – Dichiarazioni all'autorità giudiziaria	art. 377 bis	Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria

12.2 Identificazione delle attività e delle operazioni a rischio

Le attività che MIT ha individuato come sensibili, nell'ambito della fattispecie del reato di Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci, sono indicate in dettaglio nella Matrice delle Attività a Rischio-Reato conservata a cura della Società, unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

Le attività individuate quali rilevanti per la SIM sono la gestione dei rapporti:

- con i Giudici, con i loro consulenti tecnici e con i loro ausiliari, nell'ambito di procedimenti giudiziari (civili, penali, amministrativi);
- con i soggetti indagati o imputati in un procedimento penale.

Attraverso l'individuazione delle attività esposte al rischio di reato ("attività sensibili") e la strutturazione di un sistema di controllo interno volto alla prevenzione di tale rischio, MIT intende:

- da un lato, determinare una piena consapevolezza in tutti coloro che operano in nome e per conto di MIT di poter incorrere in un illecito passibile di sanzione e la cui commissione è fortemente censurata dalla SIM, in quanto sempre contraria ai suoi interessi anche quando, apparentemente, essa potrebbe trarne un vantaggio economico immediato;
- dall'altro, in virtù di un monitoraggio costante delle attività, consentire di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

12.3 Principi generali di comportamento

Coerentemente con i principi di cui alla Parte Generale del Modello Organizzativo ex D. Lgs.231/2001 e del Codice Etico adottati dalla SIM, nello svolgimento delle attività sensibili sopra citate tutti i Destinatari del Modello sono tenuti ad osservare i principi di comportamento seguenti.

La Società condanna ogni condotta che possa, in qualsivoglia modo, integrare, direttamente o indirettamente, il reato di "Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria" e/o agevolarne o favorirne la relativa commissione. In particolare, le seguenti regole di comportamento generali vietano di:

- promettere o offrire erogazioni in denaro o di altra utilità a favore di soggetti coinvolti in procedimenti giudiziari al fine di indurli ad occultare/omettere fatti che possano arrecare pene/sanzioni alla Società, proteggendo o migliorando la posizione di quest'ultima;
- indurre un soggetto a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria nel corso di un procedimento penale, attraverso minaccia o violenza (coazione fisica o morale) al fine di occultare/omettere fatti che possano arrecare pene/sanzioni alla SIM.

12.4 Procedure di controllo

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito ulteriori presidi di controllo operativi a prevenzione della commissione dei reati in oggetto, con particolare riferimento ai principali processi strumentali a presidio delle aree in oggetto:

- gli incontri, le udienze, riunioni con i Giudici, con i loro consulenti tecnici e con i loro ausiliari, nell'ambito di procedimenti giudiziari (civili, penali, amministrativi) o con i soggetti indagati o imputati in un procedimento penale sono gestiti e intrapresi solo da esponenti aziendali dotati di procura a rappresentare la società e possibilmente devono essere presenziati da due rappresentanti aziendali.

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito l'elenco dei riferimenti normativi interni e delle procedure operative adottate dalla Società all'interno dei quali la Società ha definito i presidi di controllo a prevenzione della commissione dei reati in oggetto:

- Codice Etico.

13. IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO E' IRREGOLARE (ART. 25 duodecies)

13.1 Identificazione dei reati applicabili alla SIM

In conformità a quanto previsto all' art. 6, comma 2, lett. a) del D. Lgs. 231/2001 sono state identificate le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati inclusi nel Decreto.

Nello specifico, si elencano di seguito le fattispecie di reato contemplate nel D. Lgs. 231/2001 all' art. 25 duodecies ritenute applicabili, anche se in via prudenziale, a MIT, in ragione delle attività svolte, rimandando all'Allegato 1 della Parte Generale per l'elencazione completa dei reati inclusi nella presente famiglia di reato:

Art. D. Lgs. 231/2001	**REATI PRESUPPOSTO (Codice Penale)**	
Art. 25 duodecies – Impiego di cittadini di paesi terzi il cui soggiorno è irregolare	art. 22 comma 12 bis (D. Lgs. 25 luglio 1998, n. 286)	Impiego di cittadini di Paesi terzi il cui soggiorno è irregolare aggravato da: - numero di lavoratori irregolari superiore a tre; - impiego di minori in età non lavorativa; - sottoposizione a condizioni lavorative di particolare sfruttamento, quali l'esposizione a situazioni di grave pericolo, avuto riguardo alle caratteristiche delle prestazioni da svolgere e delle condizioni di lavoro.

13.2 Identificazione delle attività e delle operazioni a rischio

Le attività che MIT ha individuato come sensibili, nell'ambito della fattispecie del reato di Impiego di cittadini di paesi terzi il cui soggiorno è irregolare, sono indicate in dettaglio nella Matrice delle Attività a Rischio-Reato conservata a cura della Società, unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

Le attività individuate quali rilevanti per la SIM sono:

- selezione e gestione dei fornitori e degli outsourcer;

Attraverso l'individuazione delle attività esposte al rischio di reato ("attività sensibili") e la strutturazione di un sistema di controllo interno volto alla prevenzione di tale rischio, MIT intende:

- da un lato, determinare una piena consapevolezza in tutti coloro che operano in nome e per conto di MIT di poter incorrere in un illecito passibile di sanzione e la cui commissione è fortemente censurata dalla SIM, in quanto sempre contraria ai suoi interessi anche quando, apparentemente, essa potrebbe trarne un vantaggio economico immediato;
- dall'altro, in virtù di un monitoraggio costante delle attività, consentire di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

13.3 Principi generali di comportamento

Coerentemente con i principi di cui alla Parte Generale del Modello Organizzativo ex D. Lgs.231/2001 e del Codice Etico adottati dalla SIM, nello svolgimento delle attività sensibili sopra citate tutti i Destinatari del Modello sono tenuti ad osservare i principi di comportamento seguenti:

- richiesta del documento di regolarità contributiva (DURC) per riscontrare la regolarità degli addetti che prestano alcune tipologie di servizi presso la Società;
- negli eventuali contratti di appalto e somministrazione di lavoro, è inserita una clausola risolutiva espressa in forza della quale l'inosservanza del divieto di assumere lavoratori stranieri privi del permesso di soggiorno, con permesso di soggiorno scaduto, non rinnovato nei tempi di legge, revocato o annullato costituirà grave inadempimento contrattuale e giustificherà la risoluzione dell'accordo, su istanza di MIT, ai sensi e per gli effetti di cui all'articolo 1456 del c.c.

13.4 Procedure di controllo

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito l'elenco dei riferimenti normativi interni e delle procedure operative adottate dalla Società all'interno dei quali la Società ha definito i presidi di controllo a prevenzione della commissione dei reati in oggetto:

- Codice Etico;
- Procedura di selezione e di gestione dei fornitori e degli *outsourcers*.

14. REATI TRIBUTARI (ART. 25 quinquiesdecies)

14.1 Identificazione dei reati applicabili alla SIM

In conformità a quanto previsto all' art. 6, comma 2, lett. a) del D. Lgs. 231/2001 sono state identificate le attività aziendali nel cui ambito possano essere potenzialmente commessi i reati inclusi nel Decreto.

Nello specifico, si elencano di seguito le fattispecie di reato contemplate nel D. Lgs. 231/2001 all' art. 25 quinquiesdecies ritenute applicabili, anche se in via prudenziale, a MIT, in ragione delle attività svolte, rimandando all'Allegato 1 della Parte Generale per l'elencazione completa dei reati inclusi nella presente famiglia di reato:

Art. D. Lgs. 231/2001	**REATI PRESUPPOSTO (Codice Penale)**	
25 quinquiesdecies – Reati Tributari	art. 2 e 3 (D. Lgs. 74/2000 con modificazioni del D. L. 124/2019)	Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti. Dichiarazione fraudolenta mediante altri artifici
	art. 8 (D. Lgs. 74/2000 con modificazioni del D. L. 124/2019)	Emissione di fatture o altri documenti per operazioni inesistenti
	art. 10 (D. Lgs. 74/2000 con modificazioni del D. L. 124/2019)	Occultamento o distruzione di documenti contabili
	art. 11 (D. Lgs. 74/2000 con modificazioni del D. L. 124/2019)	Sottrazione fraudolenta al pagamento di imposte

14.2 Identificazione delle attività e delle operazioni a rischio

Le attività che MIT ha individuato come sensibili, nell'ambito dei reati tributari, sono indicate in dettaglio nella Matrice delle Attività a Rischio-Reato conservata a cura della SIM, unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

La struttura delle fattispecie incriminatrici permette di effettuare una distinzione tra i:

- processi a rischio-reato "diretti", ossia quei processi che includono attività di natura fiscale, come la predisposizione e la presentazione delle dichiarazioni fiscali, la liquidazione e il versamento dei tributi e la tenuta e la conservazione della documentazione obbligatoria;

- processi a rischio-reato “indiretti”, ossia quei processi che, pur non includendo attività di natura fiscale, hanno riflessi su queste ultime e sono potenzialmente rilevanti per la commissione dei reati tributari (ad esempio, "approvvigionamento di beni, lavori e servizi"; “incassi e pagamenti”).

Nell’ambito dei processi a rischio-reato diretti, rientra la gestione della fiscalità, intesa come il processo di determinazione degli importi dovuti, dei versamenti e della presentazione delle dichiarazioni relative alle imposte sui redditi e sul valore aggiunto. Tale processo coinvolgerà tipicamente l’unità dell’Amministratore Delegato e Direttore Generale unitamente all’area amministrativa, gli *outsourcer*s incaricati per la parte contabile unitamente all’eventuale consulente fiscale incaricato.

In conseguenza dell’introduzione nel novero dei reati presupposto del D.Lgs. n. 231/2001 degli artt. 5 e 10-quater del D. Lgs. n. 74/2000 (rispettivamente “Omessa dichiarazione” e “Indebita compensazione”), assumono particolare rilevanza le attività di calcolo e imputazione in compensazione di eventuali crediti nei confronti dell’Erario.

Il processo di gestione amministrativo-contabile assume, inoltre, rilevanza diretta in conseguenza della previsione di cui all’art. 8, co. 1 e co. 2-bis, D.Lgs. n. 74/2000, che punisce l’emissione di fatture o altri documenti per operazioni inesistenti.

Il processo di gestione delle operazioni straordinarie, nonché i processi di gestione di cespiti e asset aziendali in genere, assumono altresì rilevanza diretta in conseguenza delle previsioni di cui all’art. 11, D. Lgs. n. 74/2000, che punisce la sottrazione fraudolenta al pagamento di imposte.

Parimenti, dalla descrizione della fattispecie di occultamento o distruzione di documenti contabili (art. 10, D. Lgs. n. 74/2000), emerge con tutta evidenza la necessità che tutte le funzioni aziendali collaborino, nello svolgimento delle proprie funzioni, all’archiviazione e alla tenuta di tutta la documentazione di cui è obbligatoria la conservazione.

Dall’analisi delle fattispecie incriminatrici introdotte nel novero dei reati presupposto della responsabilità dell’ente ex D. Lgs. n. 231/2001, emergono inoltre come rilevanti alcune condotte c.d. “preparatorie” alla commissione degli stessi, che interessano, quindi, processi a rischio-reato “indiretti”.

Le attività connesse a tali condotte insistono sui processi di natura più prettamente operativa non rientranti direttamente nel processo fiscale, ma con riflessi sullo stesso e potenzialmente rilevanti per la commissione dei reati tributari (ad esempio: "gestione acquisti di beni e servizi").

Si riporta di seguito un’esemplificazione dei principali processi a rischio reato “diretti” ed “indiretti”:

- gestione amministrativo-contabile (es: predisposizione e conservazione delle scritture contabili; raccolta, aggregazione e valutazione dei dati contabili necessari per la predisposizione del bilancio d’esercizio o rendiconto annuale, delle relazioni semestrali della SIM, nonché delle relazioni allegate al bilancio; tenuta delle scritture contabili e dei Libri Sociali e Fiscali);
- gestione della fiscalità (es: redazione delle dichiarazioni fiscali ai fini delle imposte dirette ed IVA);
- gestione delle operazioni straordinarie (ad esempio acquisizione/cessione di aziende/rami d’azienda);
- gestione dei cespiti;

- gestione della Tesoreria, dei flussi monetari e finanziari;
- gestione delle fatture attive relative ai servizi di consulenza prestati ed incasso dei corrispettivi;
- approvvigionamento di beni e servizi;
- selezione, negoziazione, stipula ed esecuzione di contratti di acquisto di servizi, ivi compresi a titolo esemplificativo i contratti di esternalizzazione, riferita a soggetti privati, con particolare riferimento alla scelta della controparte; alle attività di accertamento/attestazione di avvenuta prestazione dei servizi e di autorizzazione al pagamento. In particolare, ci si riferisce ad acquisti quali: consulenze direzionali, amministrativo-legali e collaborazioni a progetto; spese di rappresentanza; spese legate alla promozione della SIM e ai servizi ICT;
- gestione degli acquisti e pagamento delle fatture passive;
- gestione dei sistemi ICT.

Attraverso l'individuazione delle attività esposte al rischio di reato ("attività sensibili") e la strutturazione di un sistema di controllo interno volto alla prevenzione di tali rischi, MIT intende:

- da un lato, determinare una piena consapevolezza in tutti coloro che operano in nome e per conto di MIT di poter incorrere in un illecito passibile di sanzione e la cui commissione è fortemente censurata dalla SIM, in quanto sempre contraria ai suoi interessi anche quando, apparentemente, essa potrebbe trarne un vantaggio economico immediato;
- dall'altro, in virtù di un monitoraggio costante delle attività, consentire di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

14.3 Principi generali di comportamento

Coerentemente con i principi di cui alla Parte Generale del Modello Organizzativo ex D. Lgs.231/2001 e del Codice Etico adottati dalla SIM, nello svolgimento delle attività sensibili sopra citate tutti i destinatari del Modello sono tenuti ad osservare i seguenti principi di comportamento:

- agire, ciascuno secondo la propria funzione, in osservanza dei principi di correttezza, trasparenza e collaborazione, conformemente alle norme di legge, di regolamento, alle procedure aziendali esistenti, ai principi generalmente riconosciuti di tenuta della contabilità;
- stabilire in modo chiaro ed univoco la responsabilità dei diversi soggetti coinvolti nella gestione dei dati contabili, garantendo la separazione delle funzioni e la coerenza dei livelli autorizzativi, nell'ambito della rilevazione, trasmissione e aggregazione delle informazioni contabili;
- assicurare globalmente un adeguato presidio di controllo sulle registrazioni contabili routinarie e valutative, che devono essere svolte in modo accurato, corretto e veritiero, nonché rispettare i principi contabili di riferimento;
- di osservare le leggi in materia di tutela della concorrenza e del mercato e vigilare sulla perfetta osservanza delle stesse, nonché collaborare con le Autorità di Vigilanza per poter garantire la corretta trasparenza su tali aspetti.

In particolare, è fatto divieto a tutti i destinatari del Modello Organizzativo che, a qualsiasi titolo, intrattengono rapporti con clienti e/o fornitori in nome e/o per conto della società, di dar corso ai suddetti qualora la controparte chieda che la fatturazione attiva o passiva avvenga a/da soggetto diverso dalla effettiva controparte.

Oltre che astenersi dal dare corso all'esecuzione dell'operazione attiva/passiva in presenza di quanto sopra rappresentato, i suddetti soggetti dovranno di ciò prontamente informare la Funzione Compliance e l'Organismo di Vigilanza.

Parimenti, essi dovranno prontamente informare la Funzione Compliance e l'Organismo di Vigilanza tutte le volte in cui ravvisano dubbi sull'effettiva esistenza del soggetto fornitore e/o cliente e/o sull'operazione attiva o passiva risultante dalle fatture o dai documenti contabili di cui gli stessi siano venuti a conoscenza.

Inoltre, le funzioni aziendali preposte devono attentamente monitorare:

- che le fatture attive e passive siano sempre intestate alle controparti intervenute nella transazione e mai a soggetti diversi;
- eventuali operazioni "anomale", quali quelle che non appaiono vantaggiose per il cliente o per la società sotto il profilo economico o finanziario, in quanto il valore/prezzo dei beni/servizi non risulta in linea con quello normalmente praticato;
- che l'oggetto dell'attività del fornitore sia coerente con le cessioni/prestazioni di servizi fatturate;
- che la società fornitrice esista effettivamente e sia operativa, effettuando, qualora sussista qualsiasi dubbio a riguardo, verifiche e visure volte ad accertare il suo fatturato, la presenza di dipendenti, sedi, ecc.;
- che esista sempre corrispondenza scritta con il fornitore o il cliente e/o i contratti/ordini per l'effettuazione dell'operazione. A tal fine qualsiasi fattura attiva o passiva che non risulti supportata da un contratto o da un ordine scritto con il cliente/fornitore o da corrispondenza tra le parti dovrà essere prontamente comunicata alla Funzione Compliance ed all'Organismo di Vigilanza. In caso di acquisto di cespiti materiali si dovrà verificare anche la presenza di regolari documenti di trasporto dei beni;
- che tutti i pagamenti relativi a fatture attive e passive siano puntuali e tracciabili e mai effettuati avendo quale mezzo di regolazione finanziaria il denaro contante;
- l'effettiva esecuzione delle operazioni sia per quanto riguarda il lato attivo sia quello passivo.

Particolare attenzione dovrà, inoltre, essere prestata in presenza dei seguenti comportamenti tenuti dai clienti/fornitori, perché spesso celano operazioni a rischio per la commissione dei reati in esame:

- il rifiuto o l'ingiustificata riluttanza a fornire informazioni occorrenti per l'effettuazione delle operazioni o a presentare documentazione contabile di altro genere;
- la richiesta da parte di clienti di regolazione finanziaria dell'operazione con denaro contante, in sostituzione degli usuali mezzi di pagamento utilizzati;
- la richiesta di effettuazione di operazione con modalità inusuali.

È fatto obbligo a chiunque rilevi le situazioni di anomalie sopra rappresentate o altre che, a proprio parere, pongano dubbi sull'effettiva esecuzione delle operazioni rappresentate nelle fatture attive e/o passive, di darne pronta comunicazione alla Funzione Compliance ed all'Organismo di Vigilanza, astenendosi dal darvi corso.

Infine, le funzioni aziendali preposte, con il supporto, per quanto di competenza, degli *outsourcer* incaricati, devono:

- verificare la correttezza e accuratezza del calcolo delle imposte dirette e indirette dovute dalla società;
- verificare la tempestiva e corretta liquidazione delle imposte indicate nelle dichiarazioni presentate rispetto alle scadenze di legge, tenendo conto dei versamenti in acconto già effettuati;
- verificare l'avvenuto corretto versamento delle somme dovute a titolo di imposte sui redditi, di imposta sul valore aggiunto nonché delle ritenute operate dalla società quale sostituto d'imposta;
- verificare la quadratura degli importi dovuti a titolo di imposta sul valore aggiunto con i registri e i relativi conti di contabilità generale;
- verificare il rispetto dei requisiti normativi relativamente alle eventuali compensazioni d'imposta effettuate.

Qualsiasi anomalia venisse riscontrata circa la gestione degli adempimenti di carattere contabile/fiscale sopra rappresentati dovrà essere tempestivamente comunicata alla Funzione Compliance ed all'Organismo di Vigilanza.

14.4 Procedure di controllo

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito l'elenco dei riferimenti normativi interni e delle procedure operative adottate dalla Società all'interno dei quali la Società ha definito i presidi di controllo a prevenzione della commissione dei reati in oggetto:

- Codice Etico;
- Procedura di selezione e gestione dei fornitori e degli *outsourcer*;
- Policy e Procedura AML;
- Metodologia di valutazione del rischio di riciclaggio;
- Regolamento del C.d.A.