BANCA FINNAT

MODELLO ORGANIZZATIVO
AI SENSI DEL DECRETO LEGISLATIVO N. 231/01

19 SETTEMBRE 2024

INDICE

DEFINIZIONI

“Attività e/o Area a Rischio”: attività svolte dalla BANCA, nel cui ambito possono in linea di principio essere commessi i reati di cui al D.Lgs 231/2001 così come identificate nella Parte Speciale;
“Autorità di Vigilanza”: si intendono le Autorità di regolamentazione e controllo delle banche e degli altri “soggetti abilitati” ai sensi del Decreto Legislativo n° 58/1998, ossia Banca d’Italia e Consob;
“Autorità”: si intendono le Autorità di Vigilanza e altre Autorità;
“Banca” o “Banca Finnat”: Banca Finnat Euramerica S.p.A.;
“CCNL”: i Contratti Collettivi Nazionali di Lavoro stipulati dalle associazioni sindacali maggiormente rappresentative per (i) i Dipendenti delle aziende del terziario e (ii) i dirigenti dell’industria, attualmente in vigore e applicati dalla BANCA;
“Codice Di Comportamento”: Codice Interno di Comportamento e relativo allegato adottati dalla BANCA;
“Codice Etico”: Codice Etico ai sensi del Decreto Legislativo n. 231/01 adottato dalla Banca;
“Collaboratori e promotori”: coloro che agiscono in nome e/o per conto della Banca sulla base di un mandato o di altro rapporto di collaborazione;
“Consiglio di Amministrazione” o “CdA”
“Organismo di Vigilanza” o “OdV”: organismo interno preposto alla vigilanza sul funzionamento e sull’osservanza del Modello e al relativo aggiornamento;
“Consulenti”: controparti contrattuali della Banca, quali ad es. fornitori, agenti, partner, sia persone fisiche sia persone giuridiche, con cui la Banca addivenga ad una qualunque forma di collaborazione contrattualmente regolata;
“D.L.gs. 231/2001” o “Decreto”: il Decreto legislativo n. 231 dell’8 giugno 2001 e successive modifiche;
“D.L.gs. 231/2007” o “Decreto Antiriciclaggio”: il Decreto legislativo n. 231 del 21 novembre 2007 “Attuazione della direttiva 2005/60/CE concernente la prevenzione dell’utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione”;
“Destinatari”: (i) persone fisiche che rivestano funzioni di rappresentanza, amministrazione o direzione degli enti stessi o di una loro unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone fisiche che esercitino, anche di fatto, la gestione e il controllo degli enti medesimi; (ii) persone fisiche sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati;
“Dipendenti” o “Personale dipendente”: tutti i Dipendenti della Banca (compresi i dirigenti);
“Gruppo”: Gruppo Banca Finnat Euramerica S.p.A.;
“L. 146/06”: la Legge 146 del 16 marzo 2006 (Ratifica ed esecuzione della Convenzione e dei Protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'Assemblea generale il 15 novembre 2000 ed il 31 maggio 2001);
“Modello” o “MOG”: il Modello di organizzazione, gestione e controllo previsto dal Decreto e adottato dalla Banca con apposita delibera del Consiglio di Amministrazione;
“Operazione Sensibile”: operazione o atto che si colloca nell’ambito delle Aree a Rischio così come identificate nella Parte Speciale;
“Organismo Disciplinare”: l’organo competente a irrogare le sanzioni disciplinari previste dal presente Modello e specificate nel Codice Etico adottato dalla Banca;

"P.A.": la Pubblica Amministrazione, inclusi i relativi funzionari ed i soggetti incaricati di pubblico servizio, intesa in senso lato e tale da ricomprendere anche le Autorità di Vigilanza e le Autorità fiscali, oltre che la Pubblica Amministrazione di Stati esteri;
"Reati": i reati di cui gli articoli 24, 24-bis, 24-ter, 25, 25 *bis*, 25-*ter*, 25-*quater*, 25-*sexies*, 25-*septies*, 25-*octies 25-octies1, 25-novies, 25-decies, 25-quinquiesdecies, 25-septiesdecies del* Decreto ed eventuali integrazioni nonché i reati transnazionali indicati nella legge 146 del 16 marzo 2006;
"Regolamento": si intende il Regolamento dell'Organismo di Vigilanza;
"Soggetti Apicali": si intendono le persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Banca, nonché le persone che esercitano anche di fatto la gestione e il controllo della stessa.

PARTE GENERALE

1. PREMESSA

Il presente Modello di organizzazione, gestione e controllo previsto Decreto legislativo n. 231 del 2001 si integra nella normativa di governo, nelle procedure e nel sistema di controllo già esistenti ed operativi in Banca Finnat.
La Banca ha strutturato un insieme di regole e procedure che oltre a garantire il corretto funzionamento della stessa, costituiscono già di per sé uno strumento a presidio della prevenzione di comportamenti illeciti, inclusi quelli previsti dal Decreto.
In particolare quali specifici strumenti aventi finalità di controllo la Banca ha individuato:

1. Regole di governo societario (regolamento policy e processi);
2. Sistemi di controlli interni;
3. Sistema di poteri e deleghe;
4. Codice Etico.

2. FINALITA'

Nell'ambito di un'organizzazione societaria da sempre rigidamente ispirata ai temi del controllo interno e della prevenzione degli illeciti, Banca Finnat ha inteso racchiudere le norme organizzative direttamente finalizzate alla prevenzione dei reati in un documento unitario a seguito dell'entrata in vigore del Decreto.
Oltre a rispondere ad evidenti esigenze di chiarezza e di trasparenza, la predisposizione del presente documento mira a:

1. rendere noto a tutti i Destinatari che BFE condanna nella maniera più assoluta condotte contrarie a disposizioni normative, norme di vigilanza, regolamentazione interna e principi di sana e trasparente gestione dell'attività cui la Banca si ispira;
2. diffondere, all'interno della società, una scrupolosa attenzione all'osservanza degli obblighi gravanti sugli amministratori, sui dirigenti e su tutti i Dipendenti in merito alla corretta attuazione delle norme organizzative in esame, al fine di prevenire la commissione dei reati contemplati dal Decreto nell'interesse o a vantaggio dell'ente ed a consentire all'Organismo di Vigilanza il corretto svolgimento delle funzioni assegnategli;
3. informare i destinatari delle gravose sanzioni amministrative applicabili alla Banca nel caso di commissioni di reati;

4. prevenire la commissione di illeciti nell'ambito della Banca mediante il continuo controllo di tutte le aree di attività a rischio.

In questo senso, la formalizzazione di un'adeguata organizzazione, quale tangibile espressione della volontà della Banca di svolgere le proprie attività secondo linee di correttezza e di trasparenza, intende uniformarsi alle condizioni normativamente previste al riguardo, ed in particolare al disposto dell'art.6 che prevede un'ipotesi di esenzione da responsabilità se:

- l'organo dirigente dell'ente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento e l'osservanza dei modelli nonché di curare il loro aggiornamento è stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e controllo;
- le persone che hanno commesso il reato hanno agito eludendo fraudolentemente i suddetti modelli di organizzazione e gestione;
- non vi sia stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Nella stessa disposizione normativa si rinvengono inoltre i principali elementi costitutivi tenuti in considerazione ai fini dell'adozione delle presenti regole organizzative e gestionali ovvero:

- l'individuazione delle attività nel cui ambito esiste la possibilità che vengano commessi reati previsti dal Decreto;
- la previsione di obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza del Modello;
- l'introduzione di un sistema disciplinare interno idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Con l'adozione del presente Modello (in sostituzione del precedente adottato), che costituisce parte integrante della regolamentazione interna, la Banca intende pertanto adempiere agli obblighi ed agli oneri configurabili a suo carico, conformandosi ai principi ispiratori del Decreto, alle raccomandazioni delle Autorità di Vigilanza e alle linee guida delle Associazioni di categoria degli intermediari (Abi e Assosim), mantenendo sempre aggiornato il sistema dei controlli interni concernenti i reati in oggetto e valorizzando la funzione autonoma ed indipendente dell'Organismo di Vigilanza.

3. NORMATIVA DI RIFERIMENTO

Il Decreto Legislativo dell'8 giugno 2001, n. 231 attuativo della delega disposta dall'art 11, Legge n. 300/2000 ha compiuto un'innovazione epocale nel nostro ordinamento giuridico, prevedendo una forma di responsabilità diretta, di carattere punitivo, posta a carico delle persone giuridiche che sono chiamate a rispondere davanti al giudice penale per la consumazione di un reato, commesso da un proprio dirigente e/o un dipendente nell'interesse della Società.

Tale disciplina nazionale è frutto di una politica ultradecennale, comunitaria ed internazionale, di reazione alle condotte criminose degli enti, in particolare di lotta alla corruzione e di tutela degli interessi finanziari della Comunità europea. L'Italia ha così dimostrato di volersi uniformare e

costantemente adeguare alle raccomandazioni, alle risoluzioni e alle direttive adottate in sede europea, che si stanno succedendo nel corso degli anni.

Il testo del Decreto prevede l'elenco specifico, e perentorio, dei reati da cui discende la responsabilità amministrativa in capo all'ente (secondo il principio di legalità). Affinché si possa arrivare all'applicazione dell'impianto sanzionatorio è necessario che l'illecito sia stato commesso nell'interesse o a vantaggio dell'ente medesimo, e che non sia stato compiuto nell'interesse esclusivo del reo o di terzi.

Si ritiene altresì rilevante sottolineare che le sanzioni in cui potrebbero incorrere gli enti sono così altamente invalidanti, quando non addirittura preclusive per lo svolgimento dell'attività economica, che l'adozione di un MOG come indicato dal D.Lgs. n. 231/2001, seppure non abbia carattere di obbligatorietà, risulta essere una scelta strategica in una logica di prudente attività di compliance aziendale.

3.1. Fattispecie di reato

Per i reati verso i quali l'ente può essere ritenuto responsabile ai sensi del d.lgs. 231/2001 – se commessi nel suo interesse o a suo vantaggio dai soggetti qualificati ex art. 5, comma 1, del decreto stesso, si rimanda alla Parte Speciale del MOG ed. Luglio 2024 Cap. 6 "Reati 231, attività a rischio, protocolli e presidi Banca Finnat", in cui vengono rappresentati in sintesi, per ogni Reato 231 applicabile alla Banca, il numero di attività a rischio identificate e dei relativi presidi / protocolli nonché il loro riferimento all'interno della Parte Speciale del Modello.

3.2. Delitti tentati

Nelle ipotesi di commissione, nelle forme del tentativo, dei delitti rilevanti ai fini della responsabilità amministrativa degli enti, le sanzioni pecuniarie (in termini di importo) e le sanzioni interdittive (in termini di tempo) sono ridotte da un terzo alla metà, mentre è esclusa l'irrogazione di sanzioni nei casi in cui l'ente impedisca volontariamente il compimento dell'azione o la realizzazione dell'evento (art. 26 del d.lgs. 231/2001). L'esclusione di sanzioni si giustifica, in tal caso, in forza dell'interruzione di ogni rapporto di immedesimazione tra ente e soggetti che assumono di agire in suo nome e per suo conto. Si tratta di un'ipotesi particolare del c.d. "recesso attivo", previsto dall'art. 56, comma 4, c.p..

3.3. Autori del reato: soggetti in posizione apicale e soggetti sottoposti all'altrui direzione

Secondo il d.lgs. 231/2001, la società è responsabile per i reati commessi nel suo interesse o a suo vantaggio:

- da "persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dell'ente stesso" (i sopra definiti soggetti "in posizione apicale" o "apicali"; art. 5, comma 1, lett. a), del d.lgs. 231/2001);
- da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti apicali (i c.d. soggetti sottoposti all'altrui direzione o vigilanza; art. 5, comma 1, lett. b), del d.lgs. 231/2001).

Appare però opportuno ribadire che la società non risponde, per espressa previsione legislativa (art. 5, comma 2, del d.lgs. 231/2001), se le persone sopra indicate hanno agito nell'interesse esclusivo proprio o di terzi.

3.4. Modifiche all'ente

Il d.lgs. 231/2001 disciplina il regime della responsabilità patrimoniale dell'ente anche in relazione alle vicende modificative dell'ente quali la trasformazione, la fusione, la scissione e la cessione d'azienda. Secondo l'art. 27, comma 1, del d.lgs. 231/2001, dell'obbligazione per il pagamento della sanzione pecuniaria risponde l'ente con il suo patrimonio o con il fondo comune, laddove la nozione di patrimonio deve essere riferita alle società e agli enti con personalità giuridica, mentre la nozione di "fondo comune" concerne le associazioni non riconosciute. Tale previsione costituisce una forma di tutela a favore dei soci di società di persone e degli associati ad associazioni, scongiurando il rischio che gli stessi possano essere chiamati a rispondere con il loro patrimonio personale delle obbligazioni derivanti dalla comminazione all'ente delle sanzioni pecuniarie. La disposizione in esame rende, inoltre, manifesto l'intento del Legislatore di individuare una responsabilità dell'ente autonoma rispetto non solo a quella dell'autore del reato (si veda, a tale proposito, l'art. 8 del d.lgs. 231/2001) ma anche rispetto ai singoli membri della compagine sociale. Gli artt. 28-33 del d.lgs. 231/2001 regolano l'incidenza sulla responsabilità dell'ente delle vicende modificative connesse a operazioni di trasformazione, fusione, scissione e cessione di azienda. Il Legislatore ha tenuto conto di due esigenze contrapposte:

- da un lato, evitare che tali operazioni possano costituire uno strumento per eludere agevolmente la responsabilità amministrativa dell'ente;
- dall'altro, non penalizzare interventi di riorganizzazione privi di intenti elusivi. La Relazione illustrativa al d.lgs. 231/2001 afferma "Il criterio di massima al riguardo seguito è stato quello di regolare la sorte delle sanzioni pecuniarie conformemente ai principi dettati dal codice civile in ordine alla generalità degli altri debiti dell'ente originario, mantenendo, per converso, il collegamento delle sanzioni interdittive con il ramo di attività nel cui ambito è stato commesso il reato".

In caso di trasformazione, l'art. 28 del d.lgs. 231/2001 prevede (in coerenza con la natura di tale istituto che implica un semplice mutamento del tipo di società, senza determinare l'estinzione del soggetto giuridico originario) che resta ferma la responsabilità dell'ente per i reati commessi anteriormente alla data in cui la trasformazione ha avuto effetto. In caso di fusione, l'ente che risulta dalla fusione (anche per incorporazione) risponde dei reati di cui erano responsabili gli enti partecipanti alla fusione (art. 29 del d.lgs. 231/2001). L'ente risultante dalla fusione, infatti, assume tutti i diritti e obblighi delle società partecipanti all'operazione (art. 2504-bis, primo comma, c.c.) e, facendo proprie le attività aziendali, accorpa altresì quelle nel cui ambito sono stati posti in essere i reati di cui le società partecipanti alla fusione avrebbero dovuto rispondere. L'art. 30 del d.lgs. 231/2001 prevede che, nel caso di scissione parziale, la società scissa rimane responsabile per i reati commessi anteriormente alla data in cui la scissione ha avuto effetto. Gli enti beneficiari della scissione (sia totale che parziale) sono solidalmente obbligati al pagamento delle sanzioni

pecuniarie dovute dall'ente scisso per i reati commessi anteriormente alla data in cui la scissione ha avuto effetto, nel limite del valore effettivo del patrimonio netto trasferito al singolo ente.

Tale limite non si applica alle società beneficiarie, alle quali risulta devoluto, anche solo in parte, il ramo di attività nel cui ambito è stato commesso il reato. Le sanzioni interdittive relative ai reati commessi anteriormente alla data in cui la scissione ha avuto effetto si applicano agli enti cui è rimasto o è stato trasferito, anche in parte, il ramo di attività nell'ambito del quale il reato è stato commesso. L'art. 31 del d.lgs. 231/2001 prevede disposizioni comuni alla fusione e alla scissione, concernenti la determinazione delle sanzioni nell'eventualità che tali operazioni straordinarie siano intervenute prima della conclusione del giudizio. Viene chiarito, in particolare, il principio per cui il giudice deve commisurare la sanzione pecuniaria, secondo i criteri previsti dall'art. 11, comma 2, del d.lgs. 231/2001, facendo riferimento in ogni caso alle condizioni economiche e patrimoniali dell'ente originariamente responsabile, e non a quelle dell'ente cui dovrebbe imputarsi la sanzione a seguito della fusione o della scissione. In caso di sanzione interdittiva, l'ente che risulterà responsabile a seguito della fusione o della scissione potrà chiedere al giudice la conversione della sanzione interdittiva in sanzione pecuniaria, a patto che: (i) la colpa organizzativa che abbia reso possibile la commissione del reato sia stata eliminata, e (ii) l'ente abbia provveduto a risarcire il danno e messo a disposizione (per la confisca) la parte di profitto eventualmente conseguito. L'art. 32 del d.lgs. 231/2001 consente al giudice di tener conto delle condanne già inflitte nei confronti degli enti partecipanti alla fusione o dell'ente scisso al fine di configurare la reiterazione, a norma dell'art. 20 del d.lgs. 231/2001, in rapporto agli illeciti dell'ente risultante dalla fusione o beneficiario della scissione, relativi a reati successivamente commessi. Per le fattispecie della cessione e del conferimento di azienda è prevista una disciplina unitaria (art. 33 del d.lgs. 231/2001), modellata sulla generale previsione dell'art. 2560 c.c.; il cessionario, nel caso di cessione dell'azienda nella cui attività è stato commesso il reato, è solidalmente obbligato al pagamento della sanzione pecuniaria comminata al cedente, con le seguenti limitazioni:

(i) è fatto salvo il beneficio della preventiva escussione del cedente;

(ii) la responsabilità del cessionario è limitata al valore dell'azienda ceduta e alle sanzioni pecuniarie che risultano dai libri contabili obbligatori ovvero dovute per illeciti amministrativi dei quali era, comunque, a conoscenza.

Al contrario, resta esclusa l'estensione al cessionario delle sanzioni interdittive inflitte al cedente.

3.5. I modelli di organizzazione, gestione e controllo

Il D.Lgs. 231 prevede che l'adozione del MOG da parte dell'ente sia condizione necessaria, seppure non ancora sufficiente, per ottenere l'esonero della responsabilità amministrativa nel caso di commissione di reati.

L'articolo 6 del Decreto stabilisce i requisiti dei Modelli di Organizzazione, Gestione e Controllo ai fini esimenti. In particolare, è necessario che il MOG adottato risponda alle seguenti esigenze:

- individuare le aree nel cui ambito possono essere commessi i reati previsti dal Decreto (risk assessment);

- prevedere specifici protocolli/procedure diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire, nonché a formare le Unità Organizzative interessate;
- individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di tali reati;
- prevedere obblighi di informazione nei confronti dell'Organismo deputato a vigilare sul funzionamento e l'osservanza del MOG;
- introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Una volta adottato il MOG, si dovrà anche poter fornire prova che esso sia stato efficacemente attuato per prevenire reati della specie di quello verificatosi.

Il Decreto prevede una differenziazione dell'onere della prova, a seconda del soggetto che compie il reato.

Nel caso si tratti di un Soggetto apicale, la Società dovrà dimostrare di avere *adottato ed efficacemente attuato il MOG*, dando prova di avere affidato a un Organismo dell'Ente dotato di autonomi poteri di iniziativa e di controllo (Organismo di Vigilanza) il compito di vigilare sul funzionamento e sull'osservanza del MOG, anche eventualmente curandone l'aggiornamento, e che tale compito sia stato correttamente eseguito. La Società dovrà provare che il reato è stato compiuto dal Soggetto apicale eludendo fraudolentemente i modelli di organizzazione e di gestione.

Nel caso in cui, invece, il reato venga commesso da soggetti sottoposti alla direzione o alla vigilanza di un soggetto apicale, ricade sull'Autorità giudiziaria l'onere di provare l'inadeguatezza del MOG e che la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza da parte degli apicali stessi.

3.6. I modelli di organizzazione, gestione e controllo ex art. 30 del T.U. 81/08 (TUTELA DELLA SALUTE E DELLA SICUREZZA NEI LUOGHI DI LAVORO)

L'entrata in vigore del T.U. 9 aprile 2008, n. 81 "Testo Unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro" ha comportato una radicale innovazione della struttura del MOG, permettendo l'integrazione di due tipologie di professionalità, entrambe essenziali e connaturali per lo svolgimento dell'attività imprenditoriale, ma fino ad allora rimaste separate: da una parte i professionisti in materia di salute e sicurezza sui luoghi di lavoro (RSPP, consulenti, Medici Competenti, ecc.), dall'altra i professionisti in materia di responsabilità amministrativa degli enti e già coinvolti nella predisposizione del MOG.

L'art. 300 del T.U. n.81/2008, che ha modificato l'art. 25-septies del D.Lgs. n. 231/2001, ha esteso il novero dei reati presupposto per la responsabilità amministrativa degli enti, comprendendo l'omicidio colposo e le lesioni gravi o gravissime commesse per violazione o per inosservanza delle norme sulla tutela della salute e sicurezza sul lavoro. L'attribuzione della responsabilità andrà comunque subordinata alla sussistenza della "colpa specifica" a carico dell'ente (ovvero quella condotta commissiva o omissiva cui è associabile un interesse o vantaggio per l'ente medesimo).

L'articolo 30 del T.U. n. 81/2008, che richiama espressamente il D.Lgs. n. 231/2001, prevede però l'esclusione della responsabilità per l'ente che abbia *adottato ed efficacemente attuato* un Modello di Organizzazione, Gestione e Controllo idoneo ad assicurare la conformità ai requisiti ed obblighi giuridici in materia di salute e sicurezza sui luoghi di lavoro. Nello specifico, l'articolo 30 del T.U. n. 81/2008 statuisce che il Modello di Organizzazione, Gestione e Controllo, debba assicurare l'adempimento di tutti gli obblighi giuridici relativi:

- al rispetto degli standard tecnico-strutturali di legge relativi a attrezzature, impianti, luoghi di lavoro, agenti chimici, fisici e biologici;
- alle attività di valutazione dei rischi e di predisposizione delle misure di prevenzione e protezione conseguenti;
- alle attività di natura organizzativa, quali emergenze, primo soccorso, gestione degli appalti, riunioni periodiche di sicurezza, consultazioni dei rappresentanti dei lavoratori per la sicurezza;
- alle attività di sorveglianza sanitaria;
- alle attività di informazione e formazione dei lavoratori;
- alle attività di vigilanza con riferimento al rispetto delle procedure e delle istruzioni di lavoro in sicurezza da parte dei lavoratori;
- alla acquisizione di documentazioni e certificazioni obbligatorie di legge;
- alle periodiche verifiche dell'applicazione e dell'efficacia delle procedure adottate.

Per tutte le attività sopra elencate, il MOG deve prevedere idonei sistemi di registrazione dell'avvenuta attuazione e inoltre, in ragione della natura e dimensioni dell'organizzazione e dal tipo di attività svolta, un'articolazione di funzioni che assicuri le competenze tecniche e i poteri necessari per la verifica, la valutazione, la gestione e il controllo del rischio, anche in un'ottica di costante aggiornamento per il mantenimento nel tempo delle condizioni di idoneità delle misure adottate. Infine, è richiesto che il MOG preveda un idoneo sistema di controllo sull'attuazione dello stesso, nonché un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure ivi indicate.
Il riesame e l'eventuale modifica del MOG dovranno essere certamente adottati, ogni qual volta siano scoperte violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico.

4. STRUTTURA

Il Modello di Banca Finnat, adottato dal Consiglio di Amministrazione, è composto:

- dalla presente Parte Generale in cui sono riassunti i caratteri essenziali dell'organizzazione preventiva e che contiene:
  i. principi ispiratori;
  ii. la descrizione del sistema di governance e degli organismi di controllo;
  iii. l'individuazione e la nomina dell'Organismo di Vigilanza;
  iv. il sistema disciplinare ed il relativo apparato disciplinare;

- .e da una Parte Speciale in cui sono descritti i reati dalla cui commissione deriva la responsabilità della Banca.

In particolare, nella parte Speciale vengono rappresentate:

i. le analisi condotte e la metodologia utilizzata al fine di individuare le attività a rischio nel cui ambito possono essere commessi i reati di cui al D.lgs 231/2001;
ii. descritte le attività a rischio, gli ambiti di commissione dei reati ed i presidi applicati al fine di mitigare il rischio di commissione del reato stesso;
iii. per ciascun presidio sono stati individuati ruoli e responsabilità attribuendo un owner a ciascun presidio/controllo;
iv. vengono allegati gli specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire;
v. segue poi l'elenco dei reati 231 ritenuti non applicabili, con relative motivazioni che hanno portato a valutarne la non applicabilità;
vi. vengono infine descritte le modalità con cui si realizzano i flussi informativi all'Organo di Vigilanza in merito all'efficacia dei presidi dettagliati nei Protocolli adottati.

Forma altresì parte integrante del Modello il Codice Etico aziendale, nel quale sono contenuti una serie di principi generali di "deontologia aziendale" che la Banca riconosce come propri e sui quali intende richiamare l'osservanza dei propri esponenti e di tutti i suoi Dipendenti, nonché di coloro che, anche dall'esterno della Banca, cooperano al perseguimento dei fini aziendali.
Costituiscono inoltre parte integrante dell'organizzazione aziendale, anche ai fini dell'attività di prevenzione disciplinata dal presente Modello, tutte i processi aziendali approvati dall'organo avente i poteri e comunicati alle competenti funzioni aziendali.
Le disposizioni espressamente enunciate nel presente documento sono da ritenersi comunque prevalenti rispetto a qualsiasi eventuale indicazione di segno contrario, a meno di specifiche e motivate eccezioni espressamente disposte dal Consiglio di Amministrazione e comunicate all'Organismo di Vigilanza.

Al fine di garantire la dovuta chiarezza dell'impianto organizzativo e procedurale, eventuali profili di contraddizione fra le disposizioni del presente Modello e quelle enucleabili dal Codice Etico, da specifiche procedure aziendali devono essere tempestivamente segnalati all'Organismo di Vigilanza e al Consiglio di Amministrazione, il quale provvede ad uniformare le relative previsioni.

5. COMPETENZA

L'adozione del Modello, la sua approvazione e le successive modifiche e integrazioni sono rimesse al Consiglio di Amministrazione.
È peraltro riconosciuta all'Amministratore Delegato della Banca, la facoltà di apportare al testo eventuali modifiche o integrazioni, da sottoporre tempestivamente al Consiglio di Amministrazione ai fini della loro ratifica e da comunicare immediatamente all'Organismo di Vigilanza.
Nell'ambito dei poteri ad esso conferiti, l'Organismo di Vigilanza fornisce all'Amministratore Delegato ed al Consiglio di Amministratore ogni indicazione utile all'aggiornamento del Modello, anche alla luce dei profili di inosservanza o di criticità riscontrati all'esito dell'attività di vigilanza e delle eventuali modifiche normative sopravvenute.

6. PRINCIPI ISPIRATORI

Le disposizioni del Modello finalizzato a prevenire la commissione dei reati contemplati dal Decreto nell'interesse o a vantaggio dell'ente sono ispirate ai seguenti principi:

a. la separazione delle funzioni in base al quale nessuno deve poter gestire un intero processo in assoluta autonomia;
b. la verificabilità dell'autore, del contenuto, dei presupposti e delle motivazioni di ogni decisione rilevante, a garanzia della trasparenza dei processi decisionali e dell'effettività dei poteri di controllo dell'Organismo di Vigilanza;
c. la corretta conservazione dei relativi dati documentali;
d. la definizione di poteri autorizzativi coerenti con le responsabilità assegnate;
e. la responsabilizzazione dei soggetti che operano all'interno della Società, i quali devono essere resi edotti dei poteri e dei doveri connessi alle funzioni svolte;
f. l'adeguata formazione dei Dipendenti, Collaboratori e Promotori in ordine alle prescrizioni contenute nel Modello;
g. la chiarezza, la completezza, la veridicità e la tempestività negli scambi di informazione interni ed esterni alla Banca;
h. la trasparenza nella gestione delle risorse finanziarie;
i. la doverosa comunicazione all'Organismo di Vigilanza di tutte le informazioni più rilevanti.

I principi in oggetto costituiscono un punto di riferimento essenziale per la formalizzazione e per l'aggiornamento delle norme organizzative e presiedono alla corretta interpretazione delle stesse da parte dei loro destinatari.

7. DESCRIZIONE SINTETICA DELL'ATTIVITA' SOCIALE

Banca Finnat Euramerica S.p.A. rientra nella categoria di banche di minori dimensioni e/o complessità operativa, come definite dalle Disposizioni di Vigilanza (Parte prima, titolo IV, Capitolo 1, Sezione I). Essa opera all'interno del segmento delle private bank.
Banca Finnat è Capogruppo del gruppo Bancario Banca Finnat e nella sua qualità di Capogruppo esercita attività di direzione e coordinamento ai sensi della all'art. 61 del TUB.
Il Gruppo Bancario Banca Finnat si colloca tra gli intermediari di classe 3 a cui appartengono i gruppi bancari e le banche che utilizzano metodologie standardizzate con attivo individuale o consolidato pari o inferiore a 4 miliardi di Euro.
Banca Finnat è specializzata nella prestazione di servizi di investimento e advisory rivolti alla clientela privata e istituzionale. Banca Finnat ha una radicata esperienza nella gestione di patrimoni sia mobiliari che immobiliari; in particolare il modello di business che caratterizza i servizi di Private Banking è orientato a fornire servizi finanziari personalizzati e su misura a clienti ad alto patrimonio netto (HNWI) o ad elevato reddito. Oltre ai servizi di investimento vengono prestati anche i tradizionali Servizi Bancari.
Inoltre, Banca Finnat, sia direttamente sia tramite le altre società del Gruppo: Finnat Fiduciaria S.p.A., Finnat Gestioni SA Natam Man.Co. ed Investire SGR, offre un'ampia gamma di servizi e prodotti finanziari: Private Banking, Family Office, Attività Fiduciaria, servizi per gli Investitori Istituzionali, Advisory & Corporate Finance, Consulenza, Real Estate e gestione di Fondi Immobiliari.

Il Gruppo opera principalmente in Italia; due società (NATAM e Finnat Gestioni) operano rispettivamente in Lussemburgo ed in Svizzera.

8. LA GOVERNANCE SOCIETARIA E GLI ORGANISMI DI CONTROLLO

La Banca adotta il modello di amministrazione e controllo tradizionale, che si articola su due organi nominati dall'Assemblea: il Consiglio di Amministrazione, organo centrale nel sistema di governo societario cui è affidata in via esclusiva la gestione aziendale e la supervisione strategica della Banca, ed il Collegio Sindacale con funzioni di vigilanza sull'amministrazione e sull'osservanza della legge e dello Statuto sociale.
Il Consiglio di Amministrazione ha inoltre istituito tre Comitati endoconsiliari (Comitato Rischi, per le Nomine e per la Remunerazione) che hanno funzioni propositive, consultive ed istruttorie per il Consiglio stesso. L'attività di revisione legale dei conti è affidata ad una società specializzata iscritta nell'apposito Registro, incaricata dall'Assemblea dei Soci su proposta motivata del Collegio Sindacale.

8.1. Consiglio di Amministrazione

Ai sensi dell'articolo 15 dello Statuto sociale, il Consiglio di Amministrazione è composto, secondo delibera assembleare, da cinque a undici componenti, che durano in carica tre esercizi e scadono alla data dell'Assemblea convocata per l'approvazione del bilancio relativo all'ultimo esercizio della loro carica.
Lo Statuto sociale conferisce al Consiglio di Amministrazione i più ampi poteri per l'amministrazione ordinaria e straordinaria della Banca e, più segnatamente, la facoltà di compiere tutti gli atti che ritenga opportuni per l'attuazione e il raggiungimento degli scopi sociali, con esclusione dei soli atti che la legge riserva all'Assemblea.
I compiti del Consiglio di Amministrazione sono disciplinati dalla normativa *pro tempore* vigente e elencati nel funzionigramma aziendale al quale si fa espresso rinvio.

8.2. Presidente del Consiglio di Amministrazione

Al Presidente del Consiglio di Amministrazione spettano i poteri di legge e di Statuto.
Al Presidente del Consiglio di Amministrazione è attribuito il ruolo di impulso e vigilanza sul funzionamento del Consiglio di Amministrazione. A tal fine ne coordina l'attività favorendo in modo neutrale la dialettica e la partecipazione attiva dei suoi componenti, sia esecutivi che non esecutivi.
Il Presidente del Consiglio di Amministrazione assicura il bilanciamento dei poteri e si pone come interlocutore del Collegio Sindacale e dei Comitati endo – consiliari.

8.3. Organi Delegati

Il Consiglio d'Amministrazione può conferire deleghe gestionali, oltre all'Amministratore delegato, anche agli altri amministratori, coerentemente con quanto previsto nello Statuto.

8.4. Amministratore Delegato

Ferme le attribuzioni del Consiglio di amministrazione a norma di legge e di statuto, sono conferiti all'Amministratore delegato tutti i poteri necessari per l'amministrazione della Banca, con le più

ampie facoltà al riguardo; nell'ambito delle attribuzioni delegate spettano all'Amministratore delegato la rappresentanza e la firma sociale.
In via esemplificativa e non tassativa, sono conferiti all'Amministratore delegato i compiti e poteri, le facoltà e deleghe specificamente illustrati nel documento Poteri e Deleghe di volta in volta approvato dal Consiglio di Amministrazione della Banca.
L'Amministratore Delegato riferisce periodicamente circa l'attività svolta nell'ambito delle proprie deleghe.

8.5. Direttore Generale

Sono conferiti al Direttore Generale poteri separati da quelli dell'Amministratore Delegato come specificamente illustrati nel documento Poteri e Deleghe di volta in volta approvato dal Consiglio di Amministrazione della Banca.

8.6. Amministratori Indipendenti

Il Consiglio di Amministrazione è stato formato nel rispetto dei criteri indicati dal DM 169/2020 e dalla Circolare di Banca d'Italia n.285 del 17 dicembre 2013 e ss.mm.ii. Parte Prima - Recepimento in Italia della CRD IV Titolo IV - Governo societario, controlli interni, gestione dei rischi con riferimento al Capitolo 1 - Governo societario Sezione IV - Composizione e nomina degli organi sociali (di seguito "Circolare 285"). I Consiglieri qualificati come indipendenti depositano la documentazione prevista dalla Policy Fit&Proper necessaria alla valutazione del requisito di indipendenza ex art. 13 DM 169/2020.

8.7. Comitati Interni al Consiglio di Amministrazione

Al fine di favorire un efficiente sistema di informazione e consultazione che permetta al Consiglio una migliore valutazione di taluni argomenti di sua competenza, sono stati costituiti il Comitato per le Nomine, il Comitato per le Remunerazioni ed il Comitato Rischi conformemente a quanto disposto dalla Circ. 285. I Comitati sono costituiti da amministratori non esecutivi in maggioranza da indipendenti.
Il Comitato per le Nomine: svolgere funzioni di supporto nell'individuazione della composizione ottimale del Consiglio di Amministrazione, indicando le figure professionali la cui presenza possa favorirne un corretto ed efficace funzionamento
Il Comitato per le Remunerazioni: svolgere funzioni propositive e consultive per quello che concerne la remunerazione degli amministratori delegati, degli altri amministratori che ricoprono particolari cariche e dei dirigenti con responsabilità strategiche e personale rilevante di cui alle politiche di remunerazione.
Il Comitato Rischi: svolgere funzioni istruttorie propositive e consultive nei confronti della struttura operativa e nei confronti degli organi sociali e dei loro membri in merito al governo societario. Supportare le valutazioni e decisioni del Consiglio di Amministrazione in relazione al sistema dei controlli interni e di gestione dei rischi. Svolgere funzioni di supporto al Consiglio di Amministrazione nella verifica dell'interesse della Banca al compimento delle operazioni con Soggetti Collegati, nonché alla convenienza e correttezza sostanziale delle relative condizioni.

Ai lavori dei Comitati endoconsiliari, partecipa il Collegio Sindacale.
Il Responsabile della funzione Compliance è invitato a partecipare alle riunioni del Comitato per le Nomine e del Comitato per le Remunerazioni, relativamente al Comitato Rischi, il Responsabile

della Funzione Compliance riceve gli avvisi di convocazione e in caso di argomenti ritenuti di interesse, chiede al Presidente del Comitato di partecipare alla riunione
Per quanto riguardo riguarda le funzioni e i compiti assegnati a ciascun Comitato endoconsiliare si rinvia ai rispettivi regolamenti interni.

8.8. Sistema dei controlli interni

La Banca, in linea con la normativa vigente si è dotata di un Sistema di Controllo Interno idoneo a presidiare nel continuo i rischi tipici dell'attività sociale.
Il Sistema dei Controlli Interni è costituito dall'insieme delle regole, delle funzioni, delle strutture, delle risorse, dei processi e delle procedure che mirano ad assicurare una sana e prudente conduzione aziendale, coerente con gli obiettivi prefissati, attraverso l'identificazione, la misurazione, la gestione e il monitoraggio dei rischi.
Nello specifico, il Sistema dei Controlli Interni mira al conseguimento delle seguenti finalità:
a) verifica dell'attuazione delle strategie e politiche aziendali;
b) contenimento dei rischi entro i limiti indicati nel quadro di riferimento per la determinazione della propensione al rischio della Banca (Risk Appetite Framework – "RAF");
c) salvaguardia del valore delle attività e protezione dalle perdite;
d) efficacia ed efficienza dei processi aziendali;
e) affidabilità e sicurezza delle informazioni aziendali e delle procedure informatiche;
f) prevenzione del rischio che la Banca sia coinvolta, anche involontariamente, in attività illecite (con particolare riferimento a quelle connesse con il riciclaggio, l'usura ed il finanziamento del terrorismo);
g) conformità delle operazioni con la legge e la normativa di vigilanza, nonché con le politiche, i regolamenti e le procedure interne.
A tal fine il Sistema dei Controlli Interni si basa sulle seguenti tipologie di controlli:
a) controlli di linea (c.d. "controlli di primo livello"), diretti ad assicurare il corretto svolgimento delle operazioni. Essi sono effettuati dalle unità organizzative - UO (ad esempio tramite controlli di tipo gerarchico, sistematico o a campione) ovvero eseguiti nell'ambito del back office; per quanto possibile tali controlli sono incorporati nelle procedure informatiche. Le UO sono le prime responsabili della gestione dei rischi; esse devono rispettare i limiti operativi loro assegnati coerentemente con gli obiettivi di rischio e con le procedure;
b) controlli di "secondo livello" (controlli sui rischi, sulla conformità, antiriciclaggio), che hanno l'obiettivo di assicurare, tra l'altro:

1. la corretta attuazione dei processi e delle procedure;
2. il rispetto dei limiti operativi assegnati alle varie UO;
3. la conformità dell'operatività aziendale alle norme, incluse quelle di autoregolamentazione. Le funzioni preposte a tali controlli sono distinte da quelle produttive; esse concorrono alla definizione delle politiche di governo dei rischi e alla gestione dei rischi;

c) controlli di terzo livello (revisione interna), volti a individuare violazioni delle procedure e della regolamentazione nonché a valutare periodicamente la completezza, l'adeguatezza, la funzionalità (in termini di efficienza ed efficacia) e l'affidabilità del sistema dei controlli interni e del sistema informativo (ICT audit), con cadenza prefissata in relazione alla natura e all'intensità dei rischi.
Nell'organigramma e funzionigramma sono individuati in modo univoco i compiti e le responsabilità affidati al personale, anche al fine di prevenire i conflitti di interesse, garantendo la necessaria separatezza tra le funzioni operative e quelle di controllo. Le politiche e le procedure di gestione

delle risorse umane assicurano che il personale sia provvisto delle competenze e delle professionalità necessarie per l'esercizio delle responsabilità ad ognuno attribuite. Le metodologie di valutazione delle attività e passività aziendali così come i processi contabili devono essere affidabili e volti ad assicurare la corretta percezione dei rischi della Banca. La normativa interna e la documentazione è regolarmente rivista e aggiornata. Il sistema informativo, rispetto alla disciplina prevista dalla citata Circolare 285, così come i livelli di continuità operativa, devono essere adeguati e conformi a quanto previsto nella stessa Circolare.

8.8.1. La Funzione di Revisione Interna (Internal Auditing)

Le attività di revisione interna sono affidate alla Funzione Internal Auditing che riporta al Consiglio di Amministrazione della Banca.
La Funzione è dotata della necessaria autonomia e indipendenza dalle strutture operative e deve disporre di risorse e mezzi adeguati allo svolgimento del proprio incarico, opera con personale dotato delle adeguate conoscenze e competenze professionali e non ha vincoli di accesso a dati ed archivi aziendali.
L'Internal Auditing ha la responsabilità di assicurare una costante ed indipendente azione di sorveglianza sul regolare andamento dell'operatività e dei processi della Banca al fine di prevenire o rilevare l'insorgere di comportamenti o situazioni anomale e rischiose, valutando la funzionalità del complessivo sistema dei controlli interni e la sua idoneità a garantire l'efficacia e l'efficienza dei processi aziendali, la salvaguardia del valore delle attività e la protezione dalle perdite, l'affidabilità e integrità delle informazioni contabili e gestionali, la conformità delle operazioni sia alle politiche stabilite dagli Organi di governo aziendali sia alle normative interne ed esterne.
La Funzione interviene anche offrendo consulenza nei progetti avviati dalla Banca oppure nella emanazione di nuovi processi, policy, procedure e nuovi prodotti, con l'obiettivo di promuovere un sempre più adeguato sistema dei controlli interni.
I compiti e le attività della Funzione oltre che nel funzionigramma aziendale, sono definiti nell'apposito Regolamento emanato dal Consiglio di Amministrazione della Banca.
Nello svolgimento dei propri compiti, l'Internal Auditing tiene conto dei rischi insiti nelle diverse aree in funzione degli obiettivi strategici, delle informazioni desunte dalle risultanze delle attività di audit e delle priorità che ne conseguono, predispone e sottopone annualmente al Consiglio di Amministrazione, previo parere del Comitato Rischi, il Piano degli interventi sulla base del quale poi opera.
I punti di debolezza rilevati nel corso delle verifiche sono sistematicamente segnalati alle Unità Organizzative interessate per una sollecita azione di miglioramento nei cui confronti è successivamente espletata un'attività di follow-up.
Alla Funzione Internal Audit è stato attribuito il compito di controllare il regolare andamento dell'operatività della Banca e l'evoluzione dei rischi e valutare la completezza, l'adeguatezza, la funzionalità e l'affidabilità delle componenti del sistema dei controlli interni, suggerendo i possibili miglioramenti al Risk Appetite Framework ("RAF"), al processo di gestione dei rischi nonché agli strumenti di misurazione e controllo degli stessi, formulando, sulla base dei risultati dei controlli, raccomandazioni agli organi aziendali. Le principali attività della Funzione:
• controllare, anche con verifiche in loco, la regolarità delle diverse attività aziendali e il rispetto, nei diversi settori operativi, dei limiti previsti dai meccanismi di delega, nonché il pieno e corretto utilizzo delle informazioni disponibili nelle diverse attività;

• valutare la completezza, l'adeguatezza, la funzionalità, l'affidabilità delle altre componenti del sistema dei controlli interni ivi comprese le funzioni aziendali di controllo di secondo livello, del processo di gestione dei rischi e degli altri processi aziendali;
• verificare l'efficacia del processo di definizione del RAF, la coerenza interna allo schema complessivo e la conformità dell'operatività aziendale al RAF;
• verificare, in ambito ICAAP/ILAAP, l'effettiva applicazione dell'impianto regolamentare; la rispondenza dei contenuti del resoconto, verificare gli aggiornamenti e monitorare l'action plan e proporre azioni migliorative da includere nell'action plan;
• verificare l'adeguatezza, l'affidabilità complessiva e la sicurezza del sistema informativo (ICT audit) e controllare regolarmente il piano aziendale di continuità operativa;
• verificare l'adeguatezza e il corretto funzionamento dei processi aziendali, anche svolti in outsourcing, e delle metodologie di valutazione delle attività aziendali con particolare riguardo agli strumenti finanziari;
• svolgere controlli sulle funzioni operative importanti o di controllo esternalizzate; • effettuare test periodici sul funzionamento delle procedure operative e di controllo interno;
• verificare la rimozione delle anomalie riscontrate nell'operatività e nel funzionamento dei controlli;
• vigilare sul rispetto delle policy e dei regolamenti interni;
• espletare compiti d'accertamento anche con riguardo a specifiche irregolarità, ove richiesto dal Consiglio di Amministrazione, dall'Amministratore Delegato e Direttore Generale e dal Collegio Sindacale;
• comunicare in via diretta i risultati degli accertamenti e delle valutazioni effettuati agli organi aziendali e, in caso di accertamenti conclusisi con giudizi negativi o che evidenzino carenze di rilievo trasmettere gli esiti agli organi medesimi integralmente, tempestivamente e direttamente;
• assicurare agli organi aziendali adeguati flussi informativi circa gli esiti delle attività eseguite, le iniziative intraprese sulle disfunzioni accertate, nonché sulle azioni correttive da intraprendere anche con riferimento alla Società Fiduciaria del gruppo e delle altre partecipate;
• coordinarsi e scambiare flussi informativi con le altre funzioni di controllo aziendali e, con la società di revisione contabile, nonché assicurare flussi informativi verso l'Organismo di Vigilanza per le materie di competenza;
• intrattenere rapporti con gli Organi di Vigilanza per quanto riguarda le attività di competenza;
• verificare periodicamente l'adeguatezza e l'efficacia dei sistemi, dei processi, delle procedure e dei meccanismi di controllo in ambito ESG adottati dalla banca;
• in forza delle disposizioni normative, ricevere le eventuali segnalazioni riferite a violazioni whistleblowing che riguardano l'attività svolta da soggetti appartenenti alla Funzione Compliance e, ove riscontri la fondatezza, le segnala agli organi aziendali competenti per le conseguenti e opportune valutazioni;
• effettuare annualmente una verifica sulle politiche e prassi di incentivazione e portare le eventuali anomalie a conoscenza degli organi competenti ad adottare misure correttive (Assemblea dei Soci e Consiglio di Amministrazione), che ne valutano la rilevanza ai fini di una pronta informativa alla Banca d'Italia.

La Funzione Internal Audit relaziona trimestralmente gli organi aziendali sugli esiti delle attività svolte e redige e sottopone ai suddetti organi la relazione sul complesso delle attività eseguite nel corso dell'anno.

8.8.2. La Funzione Compliance

La Funzione di Compliance, posta alle dipendenze del Consiglio di Amministrazione della Banca, presiede, in linea con la disciplina della Banca d'Italia e secondo un approccio risk based, alla gestione del rischio di non conformità con riguardo all'attività aziendale, verificando tra l'altro che le procedure interne siano adeguate a prevenire tale rischio.
La Funzione Compliance è responsabile della gestione del rischio di non conformità per le norme più rilevanti, quali quelle che riguardano l'esercizio dell'attività bancaria e di intermediazione, la gestione dei conflitti di interesse, la trasparenza nei confronti della clientela e, più in generale la disciplina posta a tutela del consumatore, la sostenibilità, verificando che le procedure interne siano adeguate a prevenire tale rischio. Del rispetto dei regolamenti interni e delle normative esterne inerenti il sistema informativo. Per le altre normative, per le quali esistono specifici presidi specializzati, è responsabile, unitamente alle funzioni specialistiche incaricate, della definizione delle metodologie di valutazione del rischio di non conformità e della individuazione delle relative procedure, e procede alla verifica dell'adeguatezza delle procedure medesime a prevenire il rischio di non conformità.
Per quanto in particolare riguarda la normativa riguardante la governance societaria, d'intesa con la UO Legale, la Funzione Compliance individua le norme applicabili e i relativi rischi di non conformità, proponendo eventualmente gli interventi da apportare alla pertinente documentazione di governo, al fine di assicurare adeguato presidio dei rischi medesimi.
Dello svolgimento delle attività di competenza per il controllo dei rischi ICT e di sicurezza.
Dello svolgimento in outsourcing per la Società Fiduciaria del gruppo delle attività previste per la funzione di Compliance, laddove applicabili. Attività regolata da apposito contratto. Di assicurare l'indirizzo, il coordinamento e il controllo delle attività svolte dalle funzioni di compliance presenti nelle partecipate, secondo anche i profili dettati dal Regolamento di Gruppo.

La Funzione Compliance svolge le seguenti attività:
• definire, coadiuvato dalla Funzione Controllo rischi, la metodologia dei rischi di non conformità e valutare e controllare il rischio reputazionale, sulla base di modalità condivise;
• individuare le procedure idonee ad assicurare adeguato presidio dei rischi di non conformità identificati sulla base della metodologia di cui al paragrafo precedente; • identificare nel continuo le norme applicabili, misurare e valutare il loro impatto su processi e procedure aziendali e proporre le misure organizzative e regolamentari che si rendano necessarie per conformarsi alle normative di riferimento;
• valutare l'adeguatezza e l'efficacia delle misure adottate per rimediare alle carenze nell'adempimento degli obblighi imposti dalle normative di riferimento;
• informare le Unità organizzative competenti in ordine ad adempimenti contenuti nelle normative di riferimento, nel caso di modifiche a carattere procedurale o contrattuale;
• valutare ex ante la conformità dei progetti innovativi alla regolamentazione applicabile di tutti i progetti innovativi, ivi inclusa l'operatività in nuovi prodotti o servizi ovvero l'ingresso in nuovi mercati, che la banca intende intraprendere, avendo riguardo tra l'altro alla prevenzione e gestione dei conflitti di interesse sia tra le diverse attività svolte dalla banca, sia con riferimento ai dipendenti e agli esponenti aziendali;
• fornire consulenza ed assistenza nei confronti degli organi e delle strutture aziendali nelle materie in cui assume rilievo il rischio di non conformità, nonché collaborare nell'attività di formazione del personale circa le disposizioni applicabili alle attività svolte;

• partecipare alle riunioni dei comitati endo – consiliari, con le modalità definite nei regolamenti di ciascun comitato;
• effettuare, anche in collaborazione delle funzioni specialistiche, specifiche verifiche, nonché controlli periodici, sulle procedure aziendali per valutarne efficacia e adeguatezza rispetto all'obiettivo di prevenire il rischio di non conformità;
• verificare nel continuo il rispetto dei limiti sui conflitti di interesse previsti per le singole linee di risparmio gestito, e predisporre report informativi per le funzioni aziendali interessate;
• verificare l'analisi di conformità dei contratti di outsourcing alle normative di vigilanza;
• assicurare agli organi aziendali adeguati flussi informativi circa gli esiti delle attività eseguite, le iniziative intraprese sulle disfunzioni accertate, nonché sulle azioni correttive da intraprendere, anche con riferimento alla Società Fiduciaria del gruppo e delle altre partecipate;
• coordinarsi, e scambiare flussi informativi, con le altre funzioni di controllo aziendali e verso l'Organismo di Vigilanza per le materie di competenza;
• verificare la coerenza delle politiche e prassi di remunerazione e incentivazione aziendale;
• verificare la conformità del processo di revisione dell'ICAAP alla normativa esterna ed interna;
• monitorare l'attività di negoziazione svolta per conto terzi e conto proprio su strumenti finanziari, ai fini del rispetto della normativa sulla Market Abuse;
• gestire il sistema interno di segnalazione delle violazioni (whistleblowing). In forza delle disposizioni normative, riceve le eventuali segnalazioni e ove ne riscontri la fondatezza le segnala agli organi aziendali competenti per le conseguenti valutazioni;
• assicurare che i rischi di conformità derivanti dai rischi climatici e ambientali siano presi in debita considerazione in tutti i processi rilevanti;
• garantire e sovraintendere la conformità della Policy ESG rispetto alle disposizioni normative di volta in volta vigenti;
• gestire il registro reclami della clientela;

Con riferimento al controllo di secondo livello dei rischi ICT e di sicurezza:
• monitorare l'evoluzione normativa in ambito ICT e sicurezza;
• verificare ex ante la conformità alla regolamentazione in ambito ICT e di sicurezza della documentazione di governo della Banca, in occasione di redazione e aggiornamento della stessa, valutandone l'impatto sui processi aziendali ed assicurando i conseguenti aggiornamenti;
• concorrere alla definizione della policy di sicurezza dell'informazione;
• valutare ex ante la conformità normativa dei progetti di acquisizione e sviluppo/modifica sostanziale/change dei sistemi ICT della Banca;
• eseguire valutazioni di rischio di compliance ICT circa progetti e cambiamenti ICT;
• effettuare l'analisi di conformità alle normative dei contratti di servizio, anche in outsourcing, inclusi quelli inerenti la fornitura di servizi ICT.

8.8.3. La Funzione di Controllo dei Rischi

La Funzione Controllo Rischi, posta alle dipendenze del Consiglio di Amministrazione della Banca, costituisce un importante presidio per la gestione dei rischi connessi alle diverse attività aziendali. La Funzione è responsabile: dell'individuazione dei rischi di propria competenza connessi all'attività aziendale, della loro misurazione e monitoraggio applicando adeguate metodologie e sistemi di misurazione; dello svolgimento delle attività di competenza per il controllo dei rischi ICT e di sicurezza.

La Funzione Controllo Rischi si occupa principalmente di:

• assistere gli organi aziendali e l'alta direzione nella definizione del RAF, delle politiche di governo dei rischi e delle varie fasi che costituiscono il processo di gestione degli stessi nonché della fissazione dei limiti operativi all'assunzione delle varie tipologie di rischio. In tale contesto assicurare al Consiglio di Amministrazione flussi informativi inerenti le proprie valutazioni sui rischi connessi alle attività della banca;
• collaborare con la Direzione Amministrazione e controllo nella attività di pianificazione per quanto concerne l'analisi e la quantificazione dei rischi;
• formulare proposte per l'aggiornamento del Piano di Risanamento con riferimento a: indicatori di recovery e relative soglie di calibrazione, scenari di recovery, definizione delle metriche, sia quantitative che qualitative;
• proporre i parametri quantitativi e qualitativi necessari per la definizione del RAF, che fanno riferimento anche a scenari di stress e in caso di modifiche del contesto operativo interno ed esterno l'adeguamento di tali parametri;
• verificare l'adeguatezza del RAF e nel continuo l'adeguatezza del processo di gestione dei rischi e dei limiti operativi e, laddove opportuno, proporre l'adozione di ulteriori misure di trattamento del rischio;
• redigere periodicamente la mappa dei rischi e predisporre il Resoconto ICAAP/ILAAP in coerenza con il RAF e il Piano d risanamento;
• sviluppare, convalidare e mantenere i sistemi di misurazione e controllo dei rischi assicurandone la rispondenza ai requisiti richiesti dalla specifica normativa;
• redigere, inviare in approvazione al Consiglio di Amministrazione e trasmettere alla Banca d'Italia, entro il 30 aprile di ogni anno, la relazione dei rischi operativi e di sicurezza relativi ai servizi di pagamento;
• coadiuvare gli organi aziendali nella valutazione del rischio strategico monitorando le variabili significative anche partecipando alla definizione di una strategia in materia di rischio dell'ente e/o fornendo le proprie valutazioni sul rischio della banca o del gruppo su modifiche sostanziali o operazioni straordinarie;
• garantire che la banca disponga di processi efficaci di gestione dei rischi anche raccomandando l'apporto di miglioramenti al quadro di gestione dei rischi e misure correttive per porre rimedio a violazioni delle politiche, delle procedure e dei limiti operativi in materia di rischi;
• analizzare le esposizioni ai rischi delle linee di business e facilitare l'individuazione delle concentrazioni dei rischi;
• analizzare i rischi dei nuovi prodotti e servizi e di quelli derivanti dall'ingresso in nuovi segmenti operativi e di mercato;
• fornire pareri preventivi sulla coerenza con il RAF delle operazioni di maggiore rilievo;
• monitorare il rischio effettivo assunto dalla banca e la sua coerenza con gli obiettivi di rischio nonché il rispetto dei limiti operativi assegnati alle strutture operative in relazione all'assunzione delle varie tipologie di rischio;
• verificare nel continuo il rispetto dei limiti contrattuali previsti per le singole linee di risparmio gestito, e predisporre report informativi per le funzioni aziendali interessate;
• assicurare le attività di monitoraggio inerenti i crediti, così come dettagliate e definite nel Regolamento del Credito della banca;
• supportare il Comitato Crediti nella valutazione dei crediti anomali, fornendo le proprie raccomandazioni in merito;
• verificare l'adeguatezza e l'efficacia delle misure prese per rimediare alle carenze riscontrate nel processo di gestione del rischio;

• assicurare agli organi aziendali adeguati flussi informativi circa gli esiti delle attività eseguite, le iniziative intraprese sulle disfunzioni accertate da parte delle Unità organizzative interessate, nonché sulle azioni correttive da intraprendere e intraprese anche con riferimento alla Società Fiduciaria del gruppo e delle altre partecipate;
• coordinarsi e scambiare flussi informativi con le altre funzioni di controllo aziendali e fornire flussi informativi alla società di revisione contabile
• monitorare l'aderenza dei portafogli della Banca ai principi stabiliti per la mitigazione del rischio di sostenibilità;
• monitorare i limii contrattuali relativi agli ambiti ESG previsti nelle Gestioni patrimoniali della Banca;
• supportare il Comitato Rischi nella definizione e aggiornamento degli approcci e metodologie in ambito ESG.
Di indirizzo, coordinamento e controllo in qualità di capogruppo:
• svolgere attività di indirizzo, coordinamento e controllo sulle attività svolte dalle funzioni di risk management delle partecipate, anche attivando i necessari flussi informativi ai fini della valutazione e monitoraggio dei rischi di gruppo.

Con riferimento al controllo di secondo livello dei rischi ICT e di sicurezza:
• predisporre e aggiornare annualmente il quadro per la gestione dei rischi ICT e sicurezza, inclusi quelli derivanti da outsourcer e fornitori terzi di servizi ICT;
• concorrere alla definizione della policy di sicurezza dell'informazione, a tal fine è informata su qualsiasi attività o evento che influenzi in modo rilevante il profilo di rischio della banca (incidenti operativi o di sicurezza significativi, nonché qualsiasi modifica sostanziale ai sistemi e ai processi ICT);
• partecipare attivamente ai progetti di modifica sostanziale del sistema informativo e, in particolare, alla definizione dei processi di controllo dei rischi relativi a tali progetti, anche quelli che coinvolgono eventuali outsourcer o fornitori di servizi ICT;
• aggiornare il framework di valutazione dei rischi derivanti da progetti in ambito ICT, con focus su progetti di modifica sostanziale del sistema informativo o ai processi (in particolare, nei processi di controllo dei rischi relativi a tali progetti) e dai rischi derivanti dal proprio portafoglio di progetti ICT (gestione del piano), tenendo conto anche dei rischi che potrebbero scaturire dalle interdipendenze tra progetti diversi e dalle dipendenze di più progetti dalle stesse risorse e/o competenze;
• effettuare il monitoraggio del rischio in ambito ICT e sicurezza assunto dalla Banca e riferibile agli outsourcer informatici ed ai fornitori di servizi ICT, e della sua coerenza e aderenza con gli obiettivi di rischio posti, nonché valutarne l'adeguatezza nell'ambito del processo RAF;
• eseguire risk assessment sulla strategia ICT e formalizzarne gli esiti e le valutazioni delle nuove iniziative strategiche ICT;
• eseguire l'ICT risk assessment ai fini della valutazione del rischio ICT e di sicurezza e ad evento in caso di major incident;
• supportare la definizione delle eventuali azioni correttive e dei relativi piani di rimedio a seguito delle attività di ICT risk assessment e monitorarne l'attuazione;
• redigere annualmente il rapporto sintetico della situazione del rischio ICT e di sicurezza.

8.8.4. La Funzione Antiriciclaggio

La Funzione Antiriciclaggio, posta alle dipendenze del Consiglio di Amministrazione della Banca, ha il compito di sovrintendere all'impegno di prevenzione e gestione del rischio di riciclaggio e di finanziamento del terrorismo.
Al responsabile della Funzione sono attribuite le funzioni di "Delegato ex art. 41 del D.lgs. n. 231/2007 (delegato SOS).
La Funzione Antiriciclaggio in qualità di funzione Antiriciclaggio di gruppo:
• sovrintendere all'esercizio di valutazione dei rischi di riciclaggio condotto dalle componenti del gruppo;
• redigere una valutazione dei rischi di riciclaggio di gruppo, tenendo conto dei rischi risultanti dagli esercizi individuali, delle interrelazioni tra le singole Società del gruppo e del loro impatto sull'esposizione al rischio a livello di gruppo;
• presentare agli organi aziendali della capogruppo una relazione annuale, sull'esposizione ai rischi di riciclaggio e sulle attività della funzione Antiriciclaggio a livello di gruppo;
• elaborare e sottoporre agli organi aziendali della capogruppo procedure, metodologie e standard di gruppo in materia antiriciclaggio e garantire che le politiche e le procedure delle componenti del gruppo siano in linea con questi standard oltre che conformi alle disposizioni legislative e regolamentari in materia antiriciclaggio loro applicabili;
• stabilire flussi informativi periodici da parte di tutte le Società del gruppo.
Inerenti la Funzione Antiriciclaggio:
• identificare le norme applicabili e valutare il loro impatto sui processi e sulle procedure interne di cui la banca e la Società Fiduciaria del gruppo si sono dotate, finalizzate alla prevenzione e al contrasto dei rischi antiriciclaggio;
• collaborare alla definizione del sistema dei controlli interni e delle procedure finalizzati alla prevenzione e al contrasto dei rischi di riciclaggio;
• verificare nel continuo l'adeguatezza del processo di gestione dei rischi di riciclaggio e l'idoneità del sistema dei controlli interni e delle procedure e proporre le modifiche
organizzative e procedurali necessarie volte ad di assicurare un adeguato presidio dei rischi di riciclaggio;
• condurre verifiche sulla funzionalità del processo di segnalazione e sulla congruità delle valutazioni effettuate dal primo livello sull'operatività della clientela; • collaborare alla definizione delle politiche di governo del rischio di riciclaggio e delle varie fasi in cui si articola il processo di gestione di tale rischio;
• condurre, in raccordo con le altre funzioni aziendali interessate, l'esercizio annuale di autovalutazione dei rischi di riciclaggio a cui è esposta la Banca e la Società Fiduciaria del gruppo;
• prestare supporto e assistenza agli organi aziendali e all'alta direzione;
• valutare in via preventiva il rischio di riciclaggio connesso all'offerta di prodotti e servizi nuovi, alla modifica significativa di prodotti o servizi già offerti, all'ingresso in un nuovo mercato o all'avvio di nuove attività e raccomandare le misure necessarie per mitigare e gestire questi rischi;
• verificare l'affidabilità del sistema informativo per l'adempimento degli obblighi di adeguata verifica della clientela, conservazione dei dati e segnalazione delle operazioni sospette;
• trasmettere mensilmente alla UIF i dati aggregati concernenti l'operatività complessiva del destinatario e le comunicazioni oggettive concernenti operazioni a rischio di riciclaggio;
• informare tempestivamente gli organi aziendali di violazioni o carenze rilevanti riscontrate nell'esercizio dei relativi compiti, dello stato di avanzamento delle azioni correttive adottate e circa

l'eventuale inadeguatezza delle risorse umane e tecniche assegnate alla funzione Antiriciclaggio e la necessità di potenziarle;
• predisporre flussi informativi diretti agli organi aziendali e all'Alta Direzione;
• curare, in accordo con le altre Unità organizzative competenti in tema di formazione del personale (ed in particolare con l'Unità organizzativa Personale e Servizi Generali), la predisposizione di un adeguato piano di formazione, finalizzato ad ottenere un continuo aggiornamento del personale dipendente e dei collaboratori in tema di antiriciclaggio, da presentare all'Organo con funzioni di gestione per l'approvazione;
• coordinare le attività di rafforzata verifica della clientela nei casi in cui – per circostanze oggettive, ambientali e/o soggettive – appaia particolarmente elevato il rischio di riciclaggio;
• effettuare controlli su base campionaria finalizzati alla valutazione di adeguatezza delle procedure interne, in termini di efficacia e funzionalità delle stesse, individuando eventuali criticità e curando l'attività di follow up circa le anomalie eventualmente riscontrate;
• collaborare, nella qualità di presidio aziendale specialistico antiriciclaggio, con il Ministero dell'economia e delle finanze, Banca d'Italia, Unità di Informazione Finanziaria, Forze di polizia e altri Organi investigativi o di vigilanza
• coadiuvare il Responsabile delle operazioni sospette nel provvedere all'analisi, alla valutazione dei comportamenti inattesi pervenuti e a quella finale per l'eventuale trasmissione della operazione sospetta alla UIF;
• redigere e trasmettere agli organi aziendali il documento che definisce dettagliatamente responsabilità, compiti e modalità operative nella gestione del rischio di riciclaggio (manuale antiriciclaggio);
• presentare agli organi aziendali, con periodicità almeno annuale, la relazione sulle iniziative adottate, sulle disfunzioni accertate e sulle relative azioni correttive da intraprendere, sull'attività formativa del personale e sui risultati dell'esercizio di autovalutazione;
• redigere e trasmettere agli organi aziendali ed all'Autorità di Vigilanza adeguati flussi informativi circa gli esiti delle attività eseguite, le iniziative intraprese sulle disfunzioni accertate, nonché sulle azioni correttive da intraprendere e relazionare inoltre sull'attività di formazione del personale anche con riferimento alla Società Fiduciaria del gruppo e delle altre partecipate;
• coordinarsi e scambiare flussi informativi con le altre funzioni di controllo aziendali. In qualità di Responsabile della segnalazione delle operazioni sospette: • valutare tempestivamente le operazioni ritenute sospette ai fini della normativa antiriciclaggio e decidere in merito alla loro eventuale trasmissione alla UIF;
• comunicare l'esito della propria valutazione al responsabile della dipendenza che ha dato origine alla segnalazione;
• trasmettere alla UIF le segnalazioni ritenute fondate, omettendo l'indicazione dei nominativi dei soggetti coinvolti nella procedura di segnalazione dell'operazione;
• mantenere evidenza delle valutazioni effettuate nell'ambito della procedura, anche in caso di mancato invio della segnalazione alla UIF.

8.8.5. La Funzione Protezione dei dati personali

La Funzione Protezione dei dati personali, posta alle dipendenze del Consiglio di Amministrazione della Banca, ha il compito garantire l'efficace applicazione delle normative inerenti la protezione dei dati personali (Regolamento europeo 2016/679 / RGPD e altre disposizioni nazionali o dell'Unione europea).

La Funzione:
• aggiornare il Titolare, i Referenti interni e gli Incaricati al Trattamento sugli obblighi derivanti dalla Normativa e su eventuali evoluzioni della stessa, mediante un opportuno piano di formazione;
• fornire consulenza al Titolare ed ai Referenti interni per la redazione e l'aggiornamento della documentazione in materia di trattamento/protezione dei dati personali, collaborando con la UO Organizzazione per l'aggiornamento dei processi della banca;
• verificare ed indicare la fonte di liceità (fondamento giuridico, consenso, obbligo di legge, legittimo interesse) più idonea a garantire il rispetto della Normativa nel caso si dia inizio ad un nuovo trattamento/si adottino nuove tecnologie per la gestione dei trattamenti esistenti;
• tenere il Registro delle attività di trattamento, sotto la responsabilità del titolare, attenendosi alle istruzioni impartite da quest'ultimo;
• definire la metodologia per il rispetto dei principi di "privacy by design e by default", fornendo consulenza ai Referenti interni per lo svolgimento delle analisi di privacy by design;
• avviare le procedure per la notifica in caso di violazioni dei dati personali, al Garante ed, eventualmente, agli interessati;
• definire ed aggiornare la metodologia per lo svolgimento della DPIA, sorvegliando lo svolgimento della stessa e fornendo consulenza ai Referenti interni;
• fornire consulenza ai Referenti interni al fine di garantire che i trasferimenti di dati personali al di fuori dell'UE siano fondati sulle condizioni previste dal RGPD;
• configurare, manutenere ed evolvere il programma dei controlli periodici per la rilevazione del rispetto delle prescrizioni previste dal Regolamento Europeo, nonché di presidio delle misure di sicurezza stabilite dal Titolare;
• documentare le attività di audit con relazioni che descrivano i controlli effettuati; • assicurare agli organi aziendali adeguati flussi informativi circa gli esiti delle attività di controllo eseguite, le iniziative da intraprendere sulle non conformità accertate o su eventuali fattori critici rilevati;
• presidiare la procedura di Personal Data Breach Notification per intercettare e raccogliere segnalazioni di violazioni e valutare, insieme alla UO IT e Tecnologie ed ai Referenti interni, la gravità delle violazioni e determinare le conseguenti azioni da intraprendere. Assicurare la tenuta del Registro delle Violazioni;
• monitorare la soddisfazione delle richieste degli interessati, gestendo le richieste di esercizio dei diritti con il supporto delle Funzioni aziendali preposte;
• coordinarsi e scambiare flussi informativi con le altre funzioni di controllo aziendali.
Di indirizzo, coordinamento e controllo in qualità di capogruppo:
• trasmettere alle altre società del gruppo la Normativa interna adottata dalla Capogruppo in materia di protezione dei dati personali, nonché i relativi aggiornamenti.

8.9. Revisione del bilancio

L'Assemblea degli Azionisti conferisce l'incarico di revisione del Bilancio di esercizio e consolidato e l'incarico di revisione contabile della relazione semestrale ad una società di revisione, il cui compito consiste nell'accertamento della regolare tenuta della contabilità sociale, la corretta rilevazione dei fatti della gestione nelle scritture contabili, nonché le verifiche di corrispondenza del bilancio di esercizio con le risultanze delle scritture contabili e degli accertamenti eseguiti e la sua conformità alle norme che li disciplinano.

La società incaricata provvede ad emettere, per ciascun esercizio, una relazione sul bilancio della Banca nella quale espone il suo giudizio sulla conformità del bilancio d'esercizio alle norme che lo disciplinano.

8.10. Collegio Sindacale

A norma di statuto l'Assemblea elegge il Collegio Sindacale, costituito da tre Sindaci effettivi e da due Sindaci supplenti. Il Collegio Sindacale viene nominato secondo quanto previsto dall'art. 23 dello Statuto.
Il Collegio Sindacale, ovvero almeno due Sindaci, possono convocare l'Assemblea, previa comunicazione al Presidente del Consiglio di Amministrazione medesimo.
Il Collegio Sindacale, ovvero almeno un Sindaco, possono convocare il Consiglio di Amministrazione previa comunicazione al Presidente del Consiglio di Amministrazione medesimo.
I Sindaci durano in carica tre esercizi sociali e sono rieleggibili.

8.11. Assemblea dei Soci

L'Assemblea, regolarmente costituita, rappresenta tutti gli azionisti e le sue deliberazioni, prese in conformità della legge, obbligano gli stessi anche se non intervenuti o dissenzienti. L'Assemblea ordinaria o straordinaria, si riunisce nei modi di legge e secondo quanto stabilito dallo statuto sociale.

9. SISTEMA DISCIPLINARE ED ALTRI RIMEDI CONTRATTUALI

9.1. Pubblicità delle norme organizzative

In conformità con le finalità di prevenzione perseguite e con le garanzie previste dallo Statuto dei Lavoratori per l'adozione di sanzioni disciplinari, la Banca cura la diffusione a tutto il personale del presente Modello, mediante pubblicazione del documento nell'apposita sezione della Intranet Aziendale accessibile a tutti i Dipendenti.

9.2. Presupposti generali dell'intervento disciplinare

Banca Finnat intende sanzionare, secondo principi di adeguatezza e di proporzione, qualsiasi significativa violazione delle disposizioni e delle procedure organizzative contenute nel Modello.
Al riguardo, è opportuno sottolineare come l'applicazione delle sanzioni prescinda dalla concreta commissione di un reato e/o dall'eventuale instaurazione di un procedimento penale in quanto il sistema disciplinare adottato mira a contrastare qualsiasi violazione di disposizioni del Modello dettate ai fini della prevenzione di illeciti penali, radicando nel personale aziendale ed in tutti coloro che collaborano a qualsiasi titolo con la Banca la consapevolezza in ordine alla ferma volontà di quest'ultima di perseguire qualsiasi violazione o tentativo di violazione delle regole poste a presidio del corretto svolgimento delle mansioni e/o incarichi assegnati.

9.3. Misure nei confronti di dipendenti

La violazione da parte dei Dipendenti delle singole regole comportamentali di cui al presente Modello costituisce illecito disciplinare.
I provvedimenti disciplinari irrogabili nei riguardi dei Dipendenti – nel rispetto delle procedure previste dall'articolo 7 della legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori) ed eventuali

normative speciali applicabili – sono quelli previsti dall'apparato sanzionatorio di cui al CCNL applicato dalla Banca:

- richiamo verbale;
- rimprovero scritto;
- sospensione dal servizio e dal trattamento economico per un periodo non superiore a 10 giorni;
- licenziamento per giustificato motivo;
- licenziamento per giusta causa.

Le sanzioni e l'eventuale richiesta di risarcimento dei danni, verranno commisurate al livello di responsabilità ed autonomia del Dipendente, all'eventuale esistenza di precedenti disciplinari a carico dello stesso, all'intenzionalità del suo comportamento, nonché alla gravità del medesimo, con ciò intendendosi il livello di rischio a cui la Banca può ragionevolmente ritenersi esposta – ai sensi e per gli effetti del Decreto – a seguito della condotta censurata.

9.4. Misure nei confronti dei dirigenti

In caso di violazione, da parte di dirigenti della Banca, delle procedure previste dal presente Modello di adozione, nell'espletamento di attività connesse alle Aree a Rischio, di un comportamento non conforme alle prescrizioni del Modello stesso, la Banca provvede ad applicare nei confronti dei responsabili le misure più idonee in conformità a quanto previsto dal CCNL applicato dalla Banca.
I comportamenti sanzionabili che costituiscono violazione del presente Modello sono conformi a quelli indicati per i Dipendenti, tenuto conto del livello di responsabilità e della peculiarità del rapporto di lavoro, oltre che dell'intenzionalità e gravità del comportamento assunto.

9.5. Misure nei confronti degli Amministratori e dei Sindaci

In caso di accertamento di una probabile violazione (o del compimento di atti idonei diretti in maniera univoca a porre in essere una violazione) del Modello da parte di un membro del Consiglio di Amministrazione o del Collegio Sindacale, l'Organismo di Vigilanza (in caso di composizione differente rispetto all'Organismo di Vigilanza) provvede ad informare immediatamente l'intero Consiglio di Amministrazione ed il Collegio Sindacale sollecitando l'adozione delle opportune iniziative.

9.6. Misure nei confronti di consulenti esterni

Ogni comportamento posto in essere dai Consulenti in contrasto con le linee di condotta indicate dal presente Modello e tale da comportare il rischio di commissione di REATI potrà determinare, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico, la risoluzione del rapporto contrattuale e l'eventuale richiesta di risarcimento dei danni che ne sono conseguiti.

10. ORGANISMO DI VIGILANZA

10.1. Composizione e durata

La Banca si è dotata di un Organismo di Vigilanza di tipo collegiale, composto da tre membri, eventualmente coincidenti con i membri del Collegio Sindacale.

I componenti dell'Organismo di Vigilanza sono nominati con delibera del Consiglio di Amministrazione e svolgono le loro funzioni in autonomia ed indipendenza sino alla scadenza del loro mandato triennale.

10.2. Requisiti

L'Organismo di Vigilanza si caratterizza per la presenza dei requisiti di autonomia, indipendenza, onorabilità, professionalità e continuità di azione.
I requisiti di autonomia ed indipendenza devono essere intesi in relazione alla funzionalità dell'Organismo di Vigilanza ed ai compiti che la legge attribuisce allo stesso, assicurando all'Organismo di Vigilanza l'autonomia dell'iniziativa di controllo da ogni forma d'interferenza e/o di condizionamento esterni.
L'Organismo di Vigilanza è composto da soggetti in possesso dei comuni requisiti di onorabilità personale e di idonee competenze professionali in materia contabile, economica o giuridica, tali da consentire l'efficace svolgimento delle relative funzioni.
All'atto dell'accettazione della carica, i componenti dell'Organismo di Vigilanza si impegnano a svolgere le loro funzioni con la necessaria continuità d'azione.

10.3. Cause di ineleggibilità e di revoca

Per garantire l'indipendenza e l'autonomia dell'Organismo, non possono essere nominati come componenti dell'Organismo di Vigilanza coloro che hanno rapporti di parentela con i vertici amministrativi della Banca o di imprese ad essa collegate, né soggetti che hanno rapporti economici diretti od indiretti con la Banca o i suoi amministratori tali da condizionarne l'autonomia di giudizio.
Per garantire l'onorabilità dell'Organismo, non possono essere nominati come suoi componenti coloro che hanno riportato una condanna, o l'applicazione della pena su richiesta della parti, anche con sentenza soggetta ad impugnazione, per aver commesso uno dei reati previsti dal Decreto, o comunque ad una pena che comporti l'interdizione, anche temporanea, dai pubblici uffici ovvero dagli uffici direttivi delle persone giuridiche.
L'insorgere di simili circostanze giustifica la revoca dell'interessato e la sua conseguente sostituzione ad opera del Consiglio di Amministrazione.
Costituiscono causa di decadenza dalla carica di componente dall'Organismo di vigilanza:

- la condanna con sentenza non definitiva per aver commesso uno dei reati di cui al D.Lgs. 231/2001;
- la condanna con sentenza non definitiva ad una pena che importa l'interdizione, anche temporanea, dai pubblici uffici ovvero dagli uffici direttivi delle persone giuridiche;
- l'applicazione della pena su richiesta della parti (ancorché con sentenza soggetta ad impugnazione) per aver commesso uno dei reati di cui al D.Lgs. 231/2001.

In ogni caso la revoca da componente dell'Organismo di Vigilanza è attuata laddove sussista giusta causa ovvero se ad esempio:

- il soggetto si sia reso colpevole o abbia partecipato ad uno dei reati cui il modello si riferisce;
- sia intervenuto qualsiasi altro evento che rende impossibile la prosecuzione dell'attività.

È fatto obbligo all'interessato ed all'OdV di comunicare tempestivamente al CdA il verificarsi di qualsiasi circostanza suscettibile di incidere sulla posizione di autonomia ed indipendenza di ogni

singolo membro o comunque di pregiudicare la necessaria continuità di azione nello svolgimento delle loro funzioni.
Allo stesso modo, i componenti dell'OdV si impegnano a comunicare tempestivamente al CdA eventuali provvedimenti giurisdizionali a loro carico, ed ogni altro elemento suscettibile di integrare una delle ipotesi di revoca previste dal Modello.

10.4. Funzioni

L'OdV, le cui regole di funzionamento sono dettagliate in un apposito Regolamento approvato dal medesimo OdV, si riunisce di regola con cadenza almeno trimestrale e provvede semestralmente alla predisposizione di una relazione scritta sul funzionamento del modello, indirizzata al CdA, che contiene:

a) una valutazione generale sull'andamento dei flussi informativi a lui diretti;
b) il resoconto sull'attività svolta;
c) i profili di criticità riscontrati in termini di applicazione e di efficacia del modello organizzativo.

L'OdV verifica l'effettiva trasmissione da parte degli altri organismi societari delle comunicazioni periodiche a lui dovute, in virtù delle prescrizioni contenute nel Modello.
In caso di ritardo o di incompletezza delle informazioni, l'OdV si attiva prontamente per individuare le ragioni dell'omissione e per ottenere un tempestivo adempimento.
L'OdV stabilisce, di volta in volta, le più opportune modalità di analisi della documentazione informativa ricevuta al fine di un efficace adempimento delle proprie funzioni, che tenga in adeguata considerazione le specifiche peculiarità dei dati oggetto di verifica.
Parallelamente all'analisi dei flussi informativi periodici, l'OdV può disporre verifiche a campione sui profili ritenuti più significativi ai fini dell'attività di prevenzione e di controllo, se del caso anche richiedendo ulteriori informazioni alle funzioni aziendali coinvolte.
Ogni qualvolta l'OdV sia destinatario di una segnalazione, lo stesso procede tempestivamente alle necessarie verifiche, dando atto a verbale delle attività intraprese a tal fine.
Laddove richiesto dal dichiarante o comunque ritenuto opportuno dall'OdV, viene garantito l'anonimato agli autori delle predette segnalazioni e comunque la necessaria riservatezza, tutelando l'interessato da ogni possibile forma di ritorsione, discriminazione o penalizzazione.
Quando l'analisi dei flussi informativi, i risultati delle verifiche a campione o le specifiche segnalazioni ricevute lo rendano necessario, l'OdV provvede allo svolgimento degli opportuni accertamenti per la disamina dell'effettiva attuazione del Modello da parte delle strutture organizzative aziendali e per l'individuazione di eventuali violazioni connesse alle attività aziendali "sensibili".
A tal fine, l'OdV accede a qualsiasi documento aziendale ritenuto rilevante e dispone che i dipendenti ed i collaboratori della Banca forniscano tempestivamente le informazioni, i dati e/o le notizie loro richieste.
L'OdV propone tempestivamente all'organo dirigente o agli amministratori della Società l'adozione di eventuali sanzioni o provvedimenti disciplinari nei confronti dei soggetti che si siano resi responsabili di uno degli illeciti per cui è prevista la punibilità dell'ente dal D.Lgs. 231/2001, di gravi violazioni del Modello organizzativo o di condotte che abbiano comunque ostacolato le funzioni di controllo e di accertamento dell'Organismo.
Il Presidente dell'OdV può riferire, anche in via informale, al CdA o all'Amministratore Delegato ogniqualvolta lo ritenga opportuno.

Laddove necessario, l'OdV prende direttamente contatto con le funzioni aziendali competenti al fine di richiedere informazioni o chiarimenti, di sollecitare la trasmissione di documenti o di segnalare profili di criticità nell'attuazione del Modello.
L'OdV può scambiare informazioni con la Società di revisione e con il Collegio sindacale, qualora ritenuto necessario od opportuno nell'ambito dell'espletamento delle rispettive competenze e assunzioni di responsabilità.
In caso di scoperta di reati che mettano seriamente a rischio l'integrità patrimoniale dell'ente, il Presidente è tenuto a riferire tempestivamente per iscritto al Consiglio di amministrazione, al Collegio sindacale e, per il tramite di quest'ultimo, all'Assemblea dei soci.

10.5. Poteri dell'Organismo di Vigilanza nell'esercizio delle sue funzioni

L'Organismo ha libero accesso presso tutte le attività e strutture della Banca, senza necessità di alcun consenso preventivo, al fine di ottenere qualunque informazione o dato ritenuti necessari per l'efficace svolgimento delle sue funzioni.
Nello svolgimento delle proprie funzioni, l'Organismo può avvalersi liberamente - sotto la sua diretta sorveglianza e responsabilità - dell'ausilio di tutte le strutture della Banca ovvero ricorrere all'apporto dei consulenti esterni ritenuti più idonei.

10.6. Flussi informativi nei confronti dell'Organismo di Vigilanza

Organigramma e Sistema delle Deleghe

Affinché il Modello rifletta correttamente la struttura organizzativa della Banca e sia concretamente idoneo ad assolvere alla funzione di prevenzione di fatti illeciti attribuitagli dal Decreto l'Organismo di Vigilanza viene informato di ogni modifica intervenuta nell'Organigramma della Banca e nel sistema di deleghe in vigore.

Obblighi di segnalazione a carattere generale

Qualora i Soggetti Apicali, ovvero i Dipendenti, Collaboratori e Promotori della Banca vengano a conoscenza di situazioni, operazioni o condotte illecite poste in essere in violazione delle regole interne della Banca, o di situazioni, operazioni o condotte che possono evolversi in violazione delle regole interne della Banca, poste in essere a vantaggio della stessa o nel suo interesse, devono informare immediatamente l'Organismo di Vigilanza o, in alternativa, il responsabile della funzione di Audit, il quale provvederà a relazionare senza indugio l'Organismo di Vigilanza.
Gli autori di segnalazioni - fondate o infondate – che non dovessero risultare effettuate in mala fede devono essere garantiti con ogni mezzo da qualsiasi forma di ritorsione, discriminazione o penalizzazione, se del caso anche assicurando la riservatezza della loro identità.
L'inosservanza del richiamato dovere di segnalazione costituisce di per sé stesso illecito disciplinare.

Obblighi di comunicazione connessi alla pendenza di procedimenti penali

Salve eventuali esigenze di riservatezza connesse alla tutela del segreto istruttorio, i Soggetti Apicali, i Dipendenti, Collaboratori e Promotori della Banca sono tenuti ad informare tempestivamente l'Organismo di Vigilanza in merito ad ogni procedimento penale pendente a loro carico per fatti commessi nell'esercizio delle funzioni o dei compiti loro demandati.
L'inosservanza del richiamato dovere di comunicazione costituisce di per sé stesso illecito disciplinare.

Flussi informativi connessi alle attività sensibili

Le disposizioni organizzative e procedurali connesse alle varie tipologie di reato da prevenire disciplinano compiutamente gli ulteriori obblighi informativi verso l'Organismo di Vigilanza, la cui violazione costituisce ugualmente illecito disciplinare.

Nella sezione speciale del presente Modello Organizzativo 231 sono specificate per singolo reato le aree di attività della Banca potenzialmente interessate dallo stesso, le regole e i processi che garantiscono un presidio.

Nella Parte speciale del Modello sono indicati i flussi informativi nei confronti dell'Organismo di Vigilanza.

10.7. Risorse finanziarie e formazione

Con delibera annuale, il Consiglio di Amministrazione approva una dotazione adeguata di risorse finanziarie, proposta dall'Organismo di Vigilanza, della quale quest'ultimo potrà disporre in piena autonomia per lo svolgimento dei propri compiti ed attività.

Il Consiglio di Amministrazione provvede altresì a valutare eventuali ulteriori richieste finanziarie avanzate dell'Organismo di Vigilanza nel corso dell'anno e motivate da specifiche esigenze.

La Banca provvede infine alla formazione del personale dipendente nei modi e nei tempi ritenuti opportuni.

11. WHISTLEBLOWING

11.1. Segnalazioni verso l'Organismo di Vigilanza

Con il D.lgs. 24 del 10 marzo 2023, è stata recepita in Italia la Direttiva europea 2019/1937 (cd. Direttiva Whistleblowing). Il Decreto abroga la disciplina nazionale previgente, racchiudendo in un unico testo normativo la disciplina in materia di whistleblowing e ha come scopo principale il rafforzamento del regime di tutela dei soggetti che segnalano illeciti o attività fraudolente commesse nell'ambito dell'attività lavorativa.

Al riguardo la Banca ha messo a disposizione dei segnalanti una piattaforma informatica gestita da un terzo provider attraverso la quale effettuare segnalazioni (anche anonime) in forma sia scritta che orale. Attraverso la stessa piattaforma il segnalante può, ove lo ritenga opportuno, fissare un incontro individuale con il Responsabile dell'U.O. Compliance o suo delegato.

La Banca ha attribuito all'U.O. Compliance (gestore diretto) il compito di gestire il sistema interno di segnalazione delle violazioni whistleblowing; ricevere le eventuali segnalazioni, riscontrarne la fondatezza e segnalarle agli organi aziendali competenti per le conseguenti valutazioni.

Nei casi in cui oggetto della segnalazione siano le attività svolte dalla U.O. Compliance, oppure il soggetto segnalante o segnalato faccia parte della suddetta unità organizzativa, la segnalazione sarà inviata alla U.O. Internal Audit (gestore indiretto) che procederà con le medesime modalità operative.

Le segnalazioni devono essere circostanziate, complete ed esaustive e non possono essere basate su pregiudizi o preconcetti; devono contenere le informazioni necessarie per verificare i fatti segnalati.

Nell'ambito della gestione del canale interno Compliance:
• rilascia al segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione;
• mantiene le interlocuzioni con il segnalante,richiedere integrazioni e dare seguito alle stesse;
• riscontra la segnalazione entro tre mesi dalla data dell'avviso di ricevimento.
Ogni comunicazione con la persona segnalante deve avvenire all'interno della piattaforma al fine di conservare in modo sicuro i dati relativi a ciascuna segnalazione.
A tal fine, i soggetti individuati per la gestione delle segnalazioni hanno in dotazione una credenziale univoca di accesso alla piattaforma che non devono rivelare a terzi.
La piattaforma consente anche di tracciare l'iter di lavorazione della segnalazione. Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

A seguito dell'esame della segnalazione, ove emergano elementi di fondatezza, la Compliance informa:

- la Direzione Generale ed il responsabile della UO Personale e servizi generali;
- il Comitato di Controllo delle Violazioni (CCV) in caso di violazioni al Codice Etico;
- l'ODV in caso di violazione, fatti e/o comportamenti che possano comportare le responsabilità della Banca ex d.lgs. 231/01 secondo quanto previsto dall'art. 6.3 del Codice Etico.

La Direzione Generale decide eventuali provvedimenti sanzionatori correlati al tipo di violazione commessa, informando il responsabile della U.O. Personale e servizi generali e gli eventuali altri soggetti coinvolti nella fase di attuazione dei provvedimenti.

11.2. Presidi

Ai sensi della normativa vigente è stata formalizzata specifica Policy, nella quale sono tra l'altro enunciati i seguenti principi:

a) la Banca garantisce la riservatezza e la protezione dei dati personali del soggetto che effettua la segnalazione e del soggetto segnalato;
b) sono previsti canali specifici, autonomi e indipendenti dagli ordinari canali di comunicazione aziendale;
c) si protegge il segnalante da condotte ritorsive, discriminatorie e sleali conseguenti alla segnalazione;
d) si garantisce, in termini di rapporti gerarchici o funzionali, l'indipendenza del soggetto che riceve, esamina e valuta la segnalazione;
e) si accerta che il segnalante non abbia un conflitto di interesse correlato alla segnalazione;
f) si assicura che la decisione di eventuali provvedimenti a carico del segnalato sia assunta da funzioni aziendali differenti dal soggetto che valuta la segnalazione;

La Banca inoltre:

- ha redatto apposito processo aziendale con l'obiettivo di disciplinare in coerenza con quanto previsto nella Policy la gestione delle segnalazioni delle violazioni, identificando le fasi, i controlli, le attività e le attribuzioni di responsabilità alle Unità Organizzative/Organi coinvolti;

- mette a disposizione sull'intranet aziendale e sul sito internet della Banca informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni;
- effettua iniziative formative del personale in materia di whistleblowing.

11.3. Flussi informativi

Il responsabile della UO Compliance redige annualmente apposita relazione che contiene informazioni circa:

- il corretto svolgimento della procedura;
- le risultanze dell'attività svolta a seguito delle segnalazioni. I dati sono comunicati in versione aggregata.

La relazione è sottoposta al Consiglio di amministrazione; nel caso in cui oggetto della segnalazione siano comportamenti previsti dal D.Lgs..231/01, la relazione è inviata anche all'Organismo di Vigilanza.

La relazione, secondo quanto espressamente previsto dalla disciplina vigente, è messa a disposizione del personale della Banca e del Gruppo. Il personale ne viene a conoscenza tramite avviso di avvenuta pubblicazione su intranet aziendale, inoltrato dalla U.O. Compliance.

11.4. Sanzioni

L'art. 6 del Decreto ha introdotto il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione. In particolare, il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo, così come il mutamento di mansioni, nonché qualsiasi altra misura ritorsiva o discriminatoria.
Al riguardo, la UO Compliance, una volta ricevuta la segnalazione, e dopo aver informato gli organi interessati, nell'ambito dei propri poteri e in conformità con le vigenti disposizioni in materia di regolamentazione dei rapporti di lavoro, viene informata degli eventuali provvedimenti di carattere sanzionatorio assunti nei confronti del soggetto segnalato, in modo proporzionato alla gravità della violazione.

* * * * *