Modello di Organizzazione, gestione e controllo ai sensi del D.Lgs. n. 231/2001

Edizione: n 5

Consiglio di Amministrazione del 28 maggio 2026

Sommario

PARTE GENERALE

1. Premessa

Il presente documento descrive il Modello di Organizzazione, Gestione e Controllo adottato da Extrabanca S.p.A. (di seguito anche la "Banca" o "Extrabanca") ai sensi dell'art. 6 del Decreto Legislativo 8 giugno 2001, n. 231 (di seguito, il "D.Lgs. 231/2001" o il "Decreto").

Il Modello costituisce l'insieme dei principi, delle regole operative, dei presidi organizzativi e di controllo, nonché delle norme comportamentali adottate dalla Banca al fine di prevenire la commissione dei reati previsti dal Decreto e successive modifiche e integrazioni.

Il Modello è stato predisposto tenendo conto:

- delle Linee Guida emanate dall'Associazione Bancaria Italiana (ABI);
- delle best practice di settore;
- della struttura organizzativa e operativa della Banca;
- del sistema dei controlli interni e del corpus normativo aziendale;
- della normativa applicabile al settore bancario e finanziario.

Extrabanca riconosce l'importanza di promuovere una cultura aziendale improntata ai principi di legalità, correttezza, trasparenza, integrità e responsabilità, ritenendo tali valori elementi essenziali nello svolgimento delle attività aziendali e nei rapporti con clienti, controparti, fornitori, Autorità di Vigilanza e, più in generale, con tutti gli stakeholders.

Il Modello si integra con gli ulteriori presidi adottati dalla Banca in materia di compliance, antiriciclaggio, prevenzione della corruzione, whistleblowing, sicurezza informatica, protezione dei dati personali e continuità operativa.

2. Definizioni

Ai fini del presente Modello, i termini di seguito indicati assumono il significato riportato:

- **Banca** o **Extrabanca**: Extrabanca S.p.A..
- **Decreto** o **D.Lgs. 231/2001**: il Decreto Legislativo 8 giugno 2001, n. 231 e successive modifiche e integrazioni.
- **Attività Sensibili**: attività della Banca nel cui ambito sussiste il rischio, anche potenziale, di commissione dei reati previsti dal Decreto.
- **Pubblica Amministrazione** o **PA**: qualsiasi ente pubblico, autorità amministrativa indipendente, istituzione, amministrazione, organismo, ufficio o soggetto pubblico, italiano o estero.
- **Linee Guida ABI**: le Linee Guida emanate dall'Associazione Bancaria Italiana per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001.
- **Modello** o **MOG**: il presente Modello di Organizzazione, Gestione e Controllo adottato dalla Banca ai sensi del D.Lgs. 231/2001.
- **Codice Etico**: il Codice Etico adottato dalla Banca.
- **Organismo di Vigilanza** o **OdV**: l'organismo previsto dall'art. 6 del D.Lgs. 231/2001, dotato di autonomi poteri di iniziativa e controllo, cui è affidato il compito di vigilare sul funzionamento, sull'osservanza e sull'aggiornamento del Modello.

- **Soggetti Apicali**: i soggetti di cui all'art. 5, comma 1, lett. a), del D.Lgs. 231/2001, ossia le persone che rivestono funzioni di rappresentanza, amministrazione o direzione della Banca o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché coloro che esercitano, anche di fatto, la gestione o il controllo della stessa.
- **Soggetti Sottoposti**: i soggetti di cui all'art. 5, comma 1, lett. b), del D.Lgs. 231/2001, ossia le persone sottoposte alla direzione o vigilanza dei Soggetti Apicali.
- **Dipendenti**: i soggetti legati alla Banca da un rapporto di lavoro subordinato, parasubordinato o somministrato.
- **Partner**: le controparti contrattuali della Banca, persone fisiche o giuridiche, con cui la stessa intrattiene rapporti commerciali, professionali o di collaborazione.
- **CCNL**: il Contratto Collettivo Nazionale di Lavoro applicato dalla Banca.
- **TUF**: il Decreto Legislativo 24 febbraio 1998, n. 58 e successive modifiche e integrazioni.
- **Strumenti di attuazione del Modello**: l'insieme delle disposizioni organizzative, normative e di controllo adottate dalla Banca, tra cui, a titolo esemplificativo, statuto, organigrammi, deleghe e procure, policy, procedure, regolamenti interni, disposizioni organizzative e ulteriori presidi aziendali.

3. Struttura del documento

Il presente documento è composto da una Parte Generale e da una Parte Speciale.

La **Parte Generale** descrive la disciplina contenuta nel Decreto Legislativo 8 giugno 2001, n. 231 e successive modifiche e integrazioni (di seguito il "D.Lgs. 231/2001" o il "Decreto"), illustra i principi di governance e del sistema dei controlli interni adottati dalla Banca, individua i destinatari del Modello, disciplina il ruolo e le funzioni dell'Organismo di Vigilanza, definisce il sistema disciplinare e i flussi informativi, nonché le attività di formazione e comunicazione del Modello.

La **Parte Speciale** individua le categorie di reato ritenute rilevanti per la Banca, le attività c.d. "sensibili", ossia le attività nel cui ambito potrebbe astrattamente configurarsi il rischio di commissione dei reati previsti dal Decreto, nonché i principi di comportamento, i presidi di controllo e le misure organizzative adottate ai fini della prevenzione dei reati stessi.

Costituiscono parte integrante del Modello i seguenti **Allegati**:

- il Risk Assessment finalizzato all'individuazione delle attività sensibili e dei relativi presidi di controllo;
- il Codice Etico della Banca;
- il Regolamento dell'Organismo di Vigilanza;
- I Flussi informativi verso l'Organismo di Vigilanza;
- l'Organigramma aziendale;
- l'elenco della normativa interna in vigore;
- il Codice disciplinare aziendale

La documentazione richiamata nel presente Modello è resa disponibile secondo le modalità previste dalla normativa interna della Banca.

4. Il Decreto Legislativo 231/ 2001

4.1 Il Decreto e la normativa di riferimento

Il Decreto Legislativo 8 giugno 2001, n. 231 ha introdotto nell'ordinamento italiano la responsabilità amministrativa degli enti per determinati reati commessi, nell'interesse o a vantaggio degli stessi, da:

- soggetti che rivestono funzioni di rappresentanza, amministrazione, direzione o controllo dell'ente (c.d. "soggetti apicali");
- soggetti sottoposti alla direzione o vigilanza dei soggetti apicali.

Il Decreto si applica alle società e agli enti dotati o privi di personalità giuridica e si inserisce nel quadro delle convenzioni internazionali e delle iniziative europee in materia di contrasto alla corruzione, alla criminalità economica e ai fenomeni illeciti d'impresa.

La responsabilità prevista dal D.Lgs. 231/2001 si aggiunge a quella penale della persona fisica che ha materialmente commesso il reato e può comportare l'applicazione, nei confronti dell'ente, di:

- **sanzioni pecuniarie**: che consiste nel pagamento di una somma di denaro nella misura determinata dal Giudice, secondo i criteri di cui al D. Lgs. 231/01, fino all'importo di Euro 1.549.000,00.
- **sanzioni interdittive**: che consistono:
  - nella interdizione, definitiva o temporanea, dall'esercizio della attività;
  - nella sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
  - nel divieto, temporaneo o definitivo, di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;
  - nell'esclusione da agevolazioni, finanziamenti, contributi o sussidi e nell'eventuale revoca di quelli già concessi;
  - nel divieto, temporaneo o definitivo, di pubblicizzare beni o servizi.

- **confisca del profitto del reato**: consiste nell'acquisizione coattiva da parte dello Stato del prezzo o del profitto del reato, salvo che per la parte che può essere restituita al danneggiato e fatti in ogni caso salvi i diritti acquisiti dai terzi in buona fede.
  La responsabilità amministrativa prevista dal Decreto opera anche qualora sopravvengano vicende modificative dell'Ente quali la trasformazione, la fusione, la scissione e la cessione d'azienda.
- **pubblicazione della sentenza di condanna**: consiste nella pubblicazione della sentenza, per estratto o per intero, eseguita d'ufficio e a spese del condannato, nel sito internet del Ministero della Giustizia (per un periodo non superiore a giorni trenta e, in mancanza di determinazione da parte del Giudice, per un periodo di quindici giorni), nonché mediante affissione nel Comune ove l'Ente ha la sede principale

Il Decreto prevede, inoltre, che l'ente possa beneficiare di una forma di esonero dalla responsabilità qualora dimostri di aver adottato ed efficacemente attuato un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire la commissione dei reati previsti dalla normativa.

4.2 Le fattispecie di reato contemplate dal Decreto

L'Ente può essere chiamato a rispondere soltanto per i reati, c.d. "reati presupposto", previsti dal D.Lgs. 231/2001 o comunque da altra disposizione normativa entrata in vigore prima della commissione del fatto costituente reato.

Alla data di approvazione del presente Modello, i reati presupposto appartengono alle seguenti categorie:

- Reati commessi nei rapporti con la Pubblica Amministrazione (artt. 24 e 25);
- Reati informatici e trattamento illecito dei dati (art. 24-bis);
- Reati societari (Art. 25 ter ex D.Lgs. 231/01);
- Reati di riciclaggio, autoriciclaggio e finanziamento del terrorismo (Art. 25 octies ex D.Lgs. 231/01);
- Reati tributari (Art. 25 quinquiesdecies ex D.Lgs. 231/01);
- Reati in materia di strumenti di pagamento diversi dai contanti (Art. 25 octies.1 ex D.Lgs. 231/01);
- Delitti di criminalità organizzata (Art. 24 ter ex D.Lgs. 231/01);
- Reati in materia di violazione delle misure restrittive dell'Unione Europea (Art. 25 octies.2 ex D.Lgs. 231/01);
- Reati in materia di salute e sicurezza sul lavoro (Art. 25 septies ex D.Lgs. 231/01);
- Reati di contrabbando (Art. 25 sexiesdecies ex D.Lgs. 231/01);
- Reati transnazionali (Legge 16 marzo 2006, n. 146);
- Reati in materia di impiego di cittadini di paesi terzi il cui soggiorno è irregolare e favoreggiamento dell'immigrazione clandestina (Art. 25 duodecies ex D.Lgs. 231/01);
- Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (Art. 25 decies ex D.Lgs. 231/01);
- Delitti in materia di violazione del diritto d'autore (Art. 25 novies ex D.Lgs. 231/01);
- Delitti contro la fede pubblica, falsità in monete, carte di pubblico credito, valori di bollo e strumenti o segni di riconoscimento (Art. 25 bis ex D.Lgs. 231/01);
- Abusi di mercato (Art. 25 sexies ex D.Lgs. 231/01);
- Reati Ambientali (Art. 25 undecies ex D.Lgs. 231/01);
- Delitti contro l'industria e il commercio (Art. 25 bis.1 ex D.Lgs. 231/01);
- Razzismo e Xenofobia (Art. 25 terdecies ex D.Lgs. 231/01);
- Delitti con finalità di terrorismo o di eversione dell'ordine democratico (Art. 25 quater ex D.Lgs. 231/01);
- Pratiche di mutilazione degli organi genitali femminili (Art. 25 quater.1 ex D.Lgs. 231/01);
- Delitti contro la personalità individuale (Art. 25 quinquies ex D.Lgs. 231/01);
- Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (Art. 25 quaterdecies ex D.Lgs. 231/01);
- Delitti contro il patrimonio culturale (Art. 25 septiesdecies ex D.Lgs. 231/01);
- Riciclaggio di beni culturali e devastazione o saccheggio di beni culturali e paesaggistici (Art. 25 duodevicies ex D.Lgs. 231/01).

L'applicabilità e la rilevanza delle singole fattispecie di reato rispetto all'operatività della Banca sono valutate nell'ambito delle attività di Risk Assessment e disciplinate nella Parte Speciale del presente Modello.

4.3 Autori del reato e criteri di imputazione della responsabilità

Ai sensi dell'art. 5 del D.Lgs. 231/2001, la Banca può essere ritenuta responsabile per i reati commessi nel suo interesse o a suo vantaggio da:

- soggetti che rivestono funzioni di rappresentanza, amministrazione o direzione della Banca o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da soggetti che esercitano, anche di fatto, la gestione e il controllo della stessa (c.d. "soggetti apicali");
- soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti apicali (c.d. "soggetti subordinati").

Rientrano tra i soggetti apicali, a titolo esemplificativo:

- i componenti del Consiglio di Amministrazione;
- il Presidente;
- l'Amministratore Delegato;
- il Direttore Generale;
- i responsabili di funzioni o aree aziendali dotate di autonomia gestionale e decisionale.

Rientrano invece tra i soggetti sottoposti:

- i dipendenti;
- i collaboratori;
- i lavoratori parasubordinati;
- nonché, nei limiti previsti dalla normativa applicabile, i soggetti esterni che operano per conto della Banca sotto la direzione o vigilanza dei soggetti apicali.

La responsabilità dell'ente sussiste qualora il reato sia commesso nell'interesse o a vantaggio della Banca.
La responsabilità della Banca resta invece esclusa qualora il soggetto autore del reato abbia agito nell'esclusivo interesse proprio o di terzi.

Ai fini del Decreto:

- l'"interesse" ricorre quando il soggetto ha agito con la finalità di favorire la Banca, indipendentemente dal conseguimento effettivo del risultato;
- il "vantaggio" consiste invece nella concreta acquisizione di un'utilità o beneficio da parte della Banca, anche di natura non esclusivamente economica.

La distinzione tra soggetti apicali e soggetti sottoposti assume rilievo anche ai fini dell'accertamento della responsabilità dell'ente e del relativo onere probatorio, secondo quanto previsto dagli artt. 6 e 7 del D.Lgs. 231/2001.

4.4 Il valore esimente del Modello

Ai sensi degli artt. 6 e 7 del D.Lgs. 231/2001, l'adozione e l'efficace attuazione di un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire la commissione dei reati previsti dal Decreto costituiscono condizione per l'esonero della responsabilità amministrativa dell'ente.

In particolare, nel caso di reati commessi da soggetti apicali, la Banca non risponde qualora dimostri che:

- l'Organo Amministrativo ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello idoneo a prevenire reati della specie di quello verificatosi;
- il compito di vigilare sul funzionamento, sull'osservanza e sull'aggiornamento del Modello è stato affidato a un Organismo di Vigilanza dotato di autonomi poteri di iniziativa e controllo;
- i soggetti hanno commesso il reato eludendo fraudolentemente il Modello;
- non vi è stata omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Nel caso di reati commessi da soggetti sottoposti alla direzione o vigilanza di soggetti apicali, la responsabilità della Banca può essere esclusa qualora l'ente abbia adottato ed efficacemente attuato un Modello idoneo a prevenire reati della specie di quello verificatosi.

Ai fini dell'efficace attuazione del Modello, il D.Lgs. 231/2001 richiede:

- l'individuazione delle attività nel cui ambito possono essere commessi reati;
- la previsione di specifici protocolli e presidi di controllo diretti a programmare la formazione e l'attuazione delle decisioni della Banca;
- modalità di gestione delle risorse finanziarie idonee a prevenire la commissione dei reati;
- obblighi di informazione nei confronti dell'Organismo di Vigilanza;
- un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello.

Il presente Modello è stato predisposto tenendo conto della struttura organizzativa e operativa della Banca, delle attività svolte e dei rischi concretamente individuati nell'ambito delle attività di Risk Assessment periodicamente effettuate.

4.5 Destinatari del Modello

Sono destinatari del presente Modello di Organizzazione, Gestione e Controllo (di seguito anche il "Modello") e sono pertanto tenuti a conoscerne e rispettarne il contenuto, i principi e le disposizioni:

- i soggetti in posizione apicale, ovvero componenti del Consiglio di Amministrazione (ivi inclusi, Presidente, Amministratore Delegato e Direttore Generale) e responsabili di Area;
- i soggetti sottoposti a direzione o controllo, ovvero tutti coloro che intrattengano con la Banca un rapporto di lavoro subordinato (di seguito "Dipendenti") o parasubordinato (di seguito "Collaboratori");
- tutti coloro i quali, pur non essendo funzionalmente legati alla Banca da un rapporto di lavoro subordinato o parasubordinato, sono legati alla stessa da uno specifico contratto (di seguito anche "Soggetti Esterni").

I destinatari sono tenuti ad osservare le disposizioni contenute nel Modello, nel Codice Etico, nelle policy e procedure aziendali, nonché nelle ulteriori disposizioni organizzative adottate dalla Banca.

La Banca promuove la diffusione della conoscenza del Modello e assicura adeguate attività di informazione e formazione nei confronti dei destinatari, secondo modalità differenziate in relazione al ruolo, alle responsabilità e al livello di coinvolgimento nelle attività sensibili ai sensi del D.Lgs. 231/2001.

L'inosservanza delle disposizioni contenute nel presente Modello può comportare l'applicazione delle misure disciplinari e contrattuali previste dalla normativa vigente, dal sistema disciplinare interno e dalle clausole contrattuali adottate dalla Banca.

5. Assetto organizzativo e sistema dei controlli interni

Extrabanca adotta un assetto organizzativo e di governance coerente con la normativa applicabile al settore bancario e finanziario, nonché con i principi di sana e prudente gestione, finalizzato ad assicurare condizioni di correttezza, trasparenza e controllo nello svolgimento delle attività aziendali.

L'assetto organizzativo della Banca definisce ruoli, responsabilità, linee di riporto e meccanismi di attribuzione dei poteri, nel rispetto dei principi di segregazione delle funzioni, tracciabilità delle attività, proporzionalità dei controlli e presidio dei rischi aziendali.

La Banca si è dotata di un sistema dei controlli interni articolato e integrato, volto a garantire:

- l'efficacia e l'efficienza dei processi aziendali;
- la salvaguardia del patrimonio aziendale;
- l'affidabilità e l'integrità delle informazioni;
- il rispetto della normativa applicabile, delle disposizioni di vigilanza e della normativa interna;
- il contenimento dei rischi aziendali, inclusi i rischi di non conformità ai sensi del D.Lgs. 231/2001.

Il sistema dei controlli interni si fonda sull'insieme delle regole, delle procedure, delle strutture organizzative e dei presidi di controllo adottati dalla Banca ed è sviluppato in coerenza con la disciplina di vigilanza applicabile.

Nell'ambito del sistema dei controlli interni assumono particolare rilevanza:

- il sistema delle deleghe e procure;
- il corpus normativo interno costituito da policy, regolamenti, procedure e disposizioni organizzative;
- i controlli di linea e i controlli di secondo e terzo livello;
- i presidi in materia di compliance, antiriciclaggio, gestione dei rischi, sicurezza informatica e protezione dei dati personali;
- i flussi informativi verso gli Organi Aziendali e le funzioni di controllo;
- i sistemi di tracciabilità e conservazione della documentazione.

La Banca assicura inoltre un costante aggiornamento del proprio assetto organizzativo e del sistema dei controlli interni, anche in relazione all'evoluzione normativa, organizzativa e operativa, nonché ai rischi rilevati nell'ambito delle attività di Risk Assessment.

6. Risk Assessment e attività sensibili

Ai fini della predisposizione e dell'aggiornamento del presente Modello, Extrabanca ha effettuato un'attività di Risk Assessment finalizzata a identificare le attività e i processi aziendali nel cui ambito potrebbe sussistere il rischio di commissione dei reati previsti dal D.Lgs. 231/2001.

L'attività di analisi è stata svolta tenendo conto della struttura organizzativa della Banca, delle attività concretamente esercitate, del sistema delle deleghe e dei poteri, dei presidi di controllo esistenti, nonché della normativa applicabile al settore bancario e finanziario.

Il processo di valutazione dei rischi ha comportato:

- l'individuazione delle aree aziendali e dei processi potenzialmente esposti ai rischi-reato;

- l'analisi delle modalità operative e dei presidi di controllo esistenti;
- la valutazione del livello di rischio residuo;
- l'identificazione di eventuali interventi di rafforzamento dei controlli.

Le attività aziendali nell'ambito delle quali è stato rilevato un rischio inerente di commissione dei reati presupposto costituiscono le "attività sensibili" ai sensi del Decreto.

Gli esiti dell'attività di Risk Assessment e l'individuazione delle attività sensibili sono riportati nella Parte Speciale del Modello e nei relativi documenti di supporto, costantemente aggiornati in funzione dell'evoluzione normativa, organizzativa e operativa della Banca.

Il processo di aggiornamento del Risk Assessment viene svolto periodicamente e, comunque, in occasione di modifiche significative dell'assetto organizzativo, dell'operatività aziendale, del contesto normativo di riferimento o a seguito dell'emersione di violazioni, anomalie o criticità rilevanti ai fini del D.Lgs. 231/2001.

7. Organismo di Vigilanza

Ai sensi dell'art. 6 del D.Lgs. 231/2001, Extrabanca S.p.A. istituisce un Organismo di Vigilanza ("OdV"), dotato di autonomi poteri di iniziativa e controllo, con il compito di vigilare sul funzionamento, sull'osservanza e sull'aggiornamento del Modello.

L'OdV opera secondo principi di autonomia, indipendenza, professionalità e continuità d'azione, in conformità alla normativa vigente, alle Linee Guida ABI e agli orientamenti giurisprudenziali in materia.

7.1 Composizione e requisiti

L'Organismo di Vigilanza è nominato dal Consiglio di Amministrazione ed ha composizione collegiale. L'OdV è composto da tre membri, di cui almeno due esterni alla Banca, scelti tra soggetti in possesso di adeguati requisiti di:

- onorabilità;
- autonomia e indipendenza;
- professionalità ed esperienza nelle materie giuridiche, economico-aziendali, di compliance, controllo interno e risk management;
- continuità d'azione.

I componenti dell'OdV non devono trovarsi in situazioni di conflitto di interesse né svolgere attività incompatibili con i requisiti di indipendenza richiesti dal ruolo.

Non possono essere nominati componenti dell'OdV soggetti:

- privi dei requisiti di onorabilità previsti dalla normativa applicabile;
- destinatari di condanne, anche non definitive, per reati rilevanti ai fini del D.Lgs. 231/2001;
- che si trovino nelle condizioni di ineleggibilità o decadenza previste dall'art. 2399 c.c., ove applicabile.

7.2 Funzioni e poteri

All'Organismo di Vigilanza sono attribuiti i seguenti compiti:

- vigilare sull'effettiva applicazione e osservanza del Modello;

- verificare l'adeguatezza e l'efficacia del Modello rispetto alla struttura organizzativa e all'operatività della Banca;
- monitorare il mantenimento nel tempo dei requisiti di efficacia del Modello;
- promuovere l'aggiornamento del Modello in caso di modifiche normative, organizzative o operative rilevanti;
- verificare l'idoneità dei presidi di controllo adottati dalla Banca ai fini della prevenzione dei reati presupposto;
- ricevere, analizzare e gestire i flussi informativi e le segnalazioni rilevanti ai fini del D.Lgs. 231/2001;
- promuovere iniziative di diffusione della cultura della legalità e della compliance.

Ai fini dello svolgimento delle proprie attività, l'OdV:

- ha libero accesso alla documentazione e alle informazioni aziendali rilevanti;
- può richiedere informazioni, dati e chiarimenti alle strutture aziendali;
- può effettuare verifiche periodiche e controlli a campione sulle attività sensibili;
- può avvalersi del supporto delle funzioni aziendali competenti e, ove necessario, di consulenti esterni;
- dispone di adeguate risorse finanziarie definite dal Consiglio di Amministrazione.

Le attività dell'OdV non possono essere sindacate da altre funzioni aziendali, fermo restando il potere-dovere del Consiglio di Amministrazione di vigilare sull'adeguatezza e sull'efficacia complessiva del sistema di controllo interno e del Modello.

7.3 Flussi informativi verso l'OdV

Tutti i destinatari del Modello sono tenuti a trasmettere tempestivamente all'OdV informazioni, dati e notizie rilevanti ai fini dell'attività di vigilanza prevista dal D.Lgs. 231/2001.

Devono essere comunicate, a titolo esemplificativo:

- violazioni o presunte violazioni del Modello, del Codice Etico o delle procedure aziendali;
- comportamenti non conformi ai principi di legalità e correttezza;
- procedimenti giudiziari o indagini riguardanti reati rilevanti ai sensi del D.Lgs. 231/2001;
- ispezioni o richieste provenienti dalle Autorità di Vigilanza o da altre Autorità pubbliche;
- procedimenti disciplinari rilevanti ai fini del Decreto;
- anomalie o criticità emerse nell'ambito dei controlli interni;
- modifiche organizzative, variazioni del sistema delle deleghe e dei poteri;
- ogni altra informazione ritenuta utile ai fini dell'efficace attuazione del Modello.

L'OdV riceve inoltre specifici flussi informativi periodici dalle funzioni aziendali competenti secondo quanto previsto dalla normativa interna della Banca.

La Banca garantisce la riservatezza dell'identità del segnalante e assicura la tutela da qualsiasi forma di ritorsione, discriminazione o penalizzazione nei confronti di chi effettui segnalazioni in buona fede.

Le modalità operative di trasmissione dei flussi informativi e delle segnalazioni sono disciplinate dalle procedure aziendali e dal sistema whistleblowing adottato dalla Banca.

Le segnalazioni all'Organismo di Vigilanza possono essere trasmesse tramite gli appositi canali messi a disposizione dalla Banca, inclusa la casella di posta elettronica dedicata: organismo.vigilanza@extrabanca.eu

È inoltre possibile trasmettere comunicazioni scritte indirizzate all'Organismo di Vigilanza presso la sede della Banca.

Extrabanca S.p.A. - Via Pergolesi 2 A - 20124 MILANO [Att. Organismo di Vigilanza]

7.4 Reporting dell'OdV agli Organi Sociali

L'Organismo di Vigilanza riferisce periodicamente al Consiglio di Amministrazione e al Collegio Sindacale in merito:

- all'attività svolta;
- agli esiti delle verifiche effettuate;
- alle eventuali criticità riscontrate;
- alle violazioni rilevate;
- alle proposte di aggiornamento del Modello e di rafforzamento dei presidi di controllo.

L'OdV può inoltre riferire tempestivamente agli Organi Sociali in presenza di fatti di particolare rilevanza o urgenza.

7.5 Nomina, durata e revoca

L'Organismo di Vigilanza è nominato dal Consiglio di Amministrazione, che ne definisce composizione, durata in carica e compenso.

I componenti dell'OdV restano in carica per il periodo stabilito dal Consiglio di Amministrazione e possono essere rinnovati.

La revoca dei componenti dell'OdV può avvenire esclusivamente per giusta causa, adeguatamente motivata dal Consiglio di Amministrazione.

In caso di cessazione, decadenza o revoca di un componente, il Consiglio di Amministrazione provvede tempestivamente alla relativa sostituzione.

8. Whistleblowing

Extrabanca promuove una cultura improntata alla legalità, alla trasparenza e alla correttezza, assicurando idonei canali per la segnalazione di comportamenti, atti od omissioni che possano costituire violazioni del D.Lgs. 231/2001, del presente Modello, del Codice Etico, delle procedure interne o della normativa applicabile.

La Banca ha adottato un sistema di segnalazione interna conforme alle disposizioni della Legge n. 179/2017 e del D.Lgs. n. 24/2023, volto a garantire la corretta gestione delle segnalazioni e la tutela dei soggetti segnalanti.

Possono effettuare segnalazioni dipendenti, collaboratori, esponenti aziendali, consulenti, fornitori, partner commerciali e, più in generale, tutti i soggetti che intrattengono rapporti con la Banca.

Le segnalazioni possono essere effettuate attraverso i seguenti canali:

- tramite la piattaforma informatica dedicata disponibile sul sito istituzionale della Banca: https://www.extrabanca.com/whistleblowing/
- mediante posta ordinaria indirizzata a:

Extrabanca S.p.A. – Via Pergolesi 2, 20124 Milano – all'attenzione della Funzione Compliance e Antiriciclaggio / Internal Audit;
- mediante posta elettronica all'indirizzo dedicato: whistleblowing@extrabanca.eu;
- mediante richiesta di incontro diretto con il gestore della segnalazione, da fissarsi entro un termine ragionevole.

La piattaforma adottata dalla Banca garantisce, anche mediante strumenti di crittografia, la riservatezza dell'identità del segnalante, delle persone coinvolte o comunque menzionate nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

La Banca garantisce la tutela del segnalante contro qualsiasi forma di ritorsione, discriminazione o penalizzazione collegata, direttamente o indirettamente, alla segnalazione effettuata in buona fede.

Il gestore della segnalazione provvede all'analisi delle segnalazioni ricevute e allo svolgimento delle relative attività istruttorie, informando tempestivamente l'Organismo di Vigilanza qualora emergano profili rilevanti ai fini del D.Lgs. 231/2001.

La Banca consente altresì l'effettuazione di segnalazioni anonime, nei limiti e secondo le modalità previste dalla normativa vigente e dalla disciplina interna adottata.

Restano ferme le responsabilità previste dalla legge nei confronti di chi effettui, con dolo o colpa grave, segnalazioni infondate, diffamatorie o calunniose.

Le modalità operative di gestione delle segnalazioni, i relativi flussi informativi e le misure di tutela previste sono disciplinati dalla normativa interna adottata dalla Banca.

9. Sistema disciplinare

9.1 Funzione del sistema disciplinare

Extrabanca adotta un sistema disciplinare idoneo a sanzionare il mancato rispetto delle disposizioni contenute nel presente Modello, nel Codice Etico, nelle procedure aziendali e, più in generale, nei presidi adottati dalla Banca ai fini della prevenzione dei reati previsti dal D.Lgs. 231/2001.

L'introduzione di un sistema disciplinare costituisce requisito essenziale ai fini dell'efficace attuazione del Modello e della relativa efficacia esimente ai sensi degli artt. 6 e 7 del Decreto.

L'applicazione delle misure disciplinari prescinde dall'instaurazione o dall'esito di eventuali procedimenti penali e trova fondamento nella violazione delle regole comportamentali e dei principi di controllo previsti dal Modello.

Costituiscono violazione del Modello, a titolo esemplificativo:

- il mancato rispetto delle procedure e dei protocolli aziendali;
- la violazione dei principi contenuti nel Codice Etico;
- l'elusione dei controlli previsti dal Modello;
- la redazione o trasmissione di documentazione non veritiera;
- l'omissione di informazioni dovute all'Organismo di Vigilanza;
- l'ostacolo all'attività di controllo dell'OdV;
- la violazione delle disposizioni in materia di whistleblowing e tutela del segnalante;
- qualsiasi comportamento idoneo ad esporre la Banca al rischio di commissione dei reati previsti dal Decreto.

9.2 Principi generali di applicazione

Le sanzioni sono applicate nel rispetto della normativa vigente, delle disposizioni contrattuali applicabili e del principio di proporzionalità, tenendo conto:

- della gravità della violazione;
- del grado di dolo o colpa;
- del livello di responsabilità del soggetto coinvolto;
- dell'eventuale reiterazione della condotta;
- del rischio o danno arrecato alla Banca;
- dell'eventuale applicazione di sanzioni ai sensi del D.Lgs. 231/2001.

L'Organismo di Vigilanza è informato in merito alle violazioni rilevanti del Modello e ai provvedimenti disciplinari eventualmente adottati.

9.3 Misure nei confronti dei dipendenti

Il rispetto delle disposizioni del Modello costituisce adempimento degli obblighi derivanti dal rapporto di lavoro ai sensi degli artt. 2104 e 2106 c.c.

Nei confronti dei dipendenti trovano applicazione le misure disciplinari previste dal Contratto Collettivo Nazionale di Lavoro applicabile e dal sistema disciplinare aziendale vigente.

Le sanzioni disciplinari possono comprendere:

- richiamo verbale;
- ammonizione scritta;
- sospensione dal servizio e dal trattamento economico;
- licenziamento nei casi previsti dalla normativa e dal CCNL applicabile.

L'applicazione delle sanzioni avviene nel rispetto delle procedure previste dall'art. 7 della Legge n. 300/1970 ("Statuto dei Lavoratori").

9.4 Misure nei confronti dei dirigenti

In caso di violazione del Modello da parte di dirigenti, la Banca valuta l'adozione delle misure più idonee, nel rispetto della normativa vigente e del contratto collettivo applicabile, tenuto conto del particolare rapporto fiduciario che lega tali soggetti alla Banca.

9.5 Misure nei confronti degli amministratori e dei sindaci

In caso di violazione del Modello da parte di componenti del Consiglio di Amministrazione o del Collegio Sindacale, l'Organismo di Vigilanza informa tempestivamente gli organi competenti affinché adottino le iniziative ritenute opportune ai sensi di legge e di Statuto.

9.6 Misure nei confronti di collaboratori, consulenti, fornitori e partner

La violazione delle disposizioni del Modello da parte di collaboratori, consulenti, fornitori, outsourcer, partner commerciali o altri soggetti terzi può comportare l'applicazione delle misure previste nei relativi rapporti contrattuali, inclusa la sospensione o la risoluzione del rapporto nei casi più gravi, fatto salvo il risarcimento degli eventuali danni subiti dalla Banca.

9.7 Tutela del segnalante e violazioni whistleblowing

La Banca vieta qualsiasi forma di ritorsione, discriminazione o penalizzazione nei confronti dei soggetti che effettuino segnalazioni in buona fede ai sensi della normativa whistleblowing vigente.

Sono sanzionati:

- gli atti ritorsivi o discriminatori nei confronti del segnalante;
- le violazioni degli obblighi di riservatezza;
- l'ostacolo o il tentativo di ostacolare le segnalazioni;
- le segnalazioni effettuate con dolo o colpa grave che si rivelino infondate.

Restano ferme le responsabilità previste dalla legge nei casi di segnalazioni calunniose o diffamatorie.

10. Formazione e diffusione del Modello

Extrabanca promuove la conoscenza e la diffusione del presente Modello, del Codice Etico e dei principi previsti dal D.Lgs. 231/2001 nei confronti di tutti i destinatari, al fine di assicurare comportamenti improntati a legalità, correttezza, trasparenza e controllo dei rischi.

La Banca assicura adeguate attività di informazione, formazione e sensibilizzazione, differenziate in funzione del ruolo, delle responsabilità e delle attività svolte dai destinatari del Modello.

Le iniziative formative possono essere svolte mediante sessioni in aula, strumenti informatici, corsi e-learning, comunicazioni interne o ulteriori modalità ritenute idonee dalla Banca.

La partecipazione alle attività formative previste dalla Banca può essere considerata obbligatoria per i destinatari interessati.

Il Modello, il Codice Etico e la documentazione rilevante ai fini del D.Lgs. 231/2001 sono resi disponibili attraverso i canali di comunicazione interna adottati dalla Banca e con modalità idonee a garantirne la conoscibilità da parte dei destinatari.

La Banca promuove inoltre la diffusione dei principi del Modello nei confronti di collaboratori esterni, consulenti, fornitori e partner commerciali, anche mediante specifiche clausole contrattuali o informative dedicate.

PARTE SPECIALE

1. Finalità della Parte Speciale

La presente Parte Speciale del Modello di Organizzazione, Gestione e Controllo adottato da Extrabanca S.p.A. ai sensi del D.Lgs. 231/2001 ha la finalità di:

- individuare le attività aziendali considerate sensibili ai fini della possibile commissione dei reati presupposto previsti dal Decreto;
- identificare le categorie di reato ritenute rilevanti in relazione all'operatività della Banca;

- definire i principi di comportamento, i protocolli e i presidi di controllo adottati dalla Banca a prevenzione dei rischi di reato;
- disciplinare i flussi informativi e gli obblighi di segnalazione verso l'Organismo di Vigilanza;
- supportare la diffusione di una cultura aziendale improntata ai principi di legalità, correttezza, trasparenza, responsabilità e tracciabilità delle attività aziendali.

La Parte Speciale è stata predisposta tenendo conto:

- delle risultanze delle attività di Risk Assessment svolte dalla Banca;
- della struttura organizzativa, dei processi operativi e dell'effettiva operatività di Extrabanca;
- del sistema dei controlli interni e della normativa aziendale vigente;
- delle Linee Guida ABI in materia di responsabilità amministrativa degli enti;
- della normativa applicabile al settore bancario e finanziario.

Le attività sensibili individuate sono state analizzate con riferimento alle categorie di reato ritenute concretamente applicabili alla realtà operativa della Banca, tenendo conto del livello di rischio inerente, dei presidi di controllo esistenti e del rischio residuo risultante dall'attività di valutazione effettuata.

Per ciascuna categoria di reato rilevante sono individuati:

- i processi e le attività sensibili;
- le funzioni aziendali coinvolte;
- i possibili profili di rischio;
- i principi generali di comportamento;
- i principali presidi organizzativi, procedurali e di controllo adottati dalla Banca;
- gli eventuali flussi informativi verso l'Organismo di Vigilanza.

La presente Parte Speciale deve essere letta congiuntamente:

- alla Parte Generale del Modello;
- al Codice Etico;
- alle policy, procedure e disposizioni organizzative aziendali;
- alla documentazione di Risk Assessment e ai relativi allegati.

Le disposizioni contenute nella presente Parte Speciale si applicano a tutti i destinatari del Modello, i quali sono tenuti ad osservare i principi e le regole di comportamento ivi previsti nello svolgimento delle attività di rispettiva competenza.

2. Metodologia di Risk Assessment

La Banca ha effettuato un'attività di Risk Assessment finalizzata a individuare le attività nel cui ambito possono essere astrattamente commessi i reati previsti dal D.Lgs. 231/2001, nonché a valutare l'adeguatezza dei presidi organizzativi e di controllo esistenti.

L'attività di analisi è stata svolta tenendo conto:

- della struttura organizzativa e operativa della Banca;
- delle caratteristiche dei processi aziendali;
- delle deleghe e dei poteri attribuiti;
- del sistema dei controlli interni;
- della normativa applicabile al settore bancario e finanziario;

- delle Linee Guida ABI;
- delle risultanze delle attività di controllo svolte dalle funzioni aziendali competenti.

Il Risk Assessment è stato sviluppato attraverso:

- l'analisi della documentazione organizzativa e normativa interna;
- l'esame dei processi aziendali e delle attività operative;
- incontri e interviste con i responsabili delle funzioni aziendali;
- l'individuazione delle attività sensibili e dei possibili scenari di rischio;
- la valutazione dei presidi di controllo esistenti.

Per ciascuna categoria di reato rilevante sono stati individuati:

- i processi e le attività sensibili;
- le funzioni coinvolte;
- i potenziali rischi-reato;
- i presidi organizzativi, procedurali e di controllo esistenti;
- il livello di rischio inerente;
- il livello di rischio residuo.

La valutazione del rischio inerente è effettuata mediante attribuzione di:

- un indice di probabilità di accadimento;
- un indice di impatto potenziale;

secondo criteri qualitativi e quantitativi definiti dalla Banca.

Il rischio inerente è determinato attraverso una matrice di valutazione che combina probabilità e impatto.

Successivamente, i presidi di controllo esistenti sono valutati mediante attribuzione di un coefficiente di mitigazione, volto a misurare l'efficacia del sistema dei controlli interni nella prevenzione dei rischi di reato.

Il rischio residuo è determinato tenendo conto:

- del livello di rischio inerente;
- del grado di formalizzazione delle procedure;
- della segregazione dei compiti;
- della tracciabilità delle operazioni;
- dei controlli di linea e di secondo livello;
- dei flussi informativi verso le funzioni di controllo e l'Organismo di Vigilanza;
- dell'efficacia complessiva dei presidi organizzativi adottati dalla Banca.

Le risultanze dell'attività di Risk Assessment sono formalizzate in apposita matrice dei rischi, aggiornata periodicamente e comunque in occasione di:

- modifiche normative rilevanti;
- variazioni dell'assetto organizzativo o operativo della Banca;
- introduzione di nuovi prodotti, servizi o processi;
- modifiche del sistema dei controlli interni;
- emersione di violazioni del Modello o di nuove aree di rischio.

Le risultanze del Risk Assessment costituiscono il presupposto per la definizione e l'aggiornamento dei protocolli di controllo e delle misure di prevenzione previste dal presente Modello.

Le risultanze dell'attività di Risk Assessment, incluse le attività sensibili individuate, i presidi di controllo adottati dalla Banca e i livelli di rischio residuo associati alle singole categorie di reato, sono riportate nella matrice dei rischi allegata al presente Modello.

Le categorie di reato classificate a rischiosità inerente trascurabile possono non presentare specifiche attività sensibili o processi dedicati nella matrice di Risk Assessment, qualora l'analisi svolta abbia evidenziato un livello di esposizione non significativo rispetto all'operatività della Banca.

3. Reati rilevanti, attività sensibili e presidi di controllo

Sulla base delle risultanze dell'attività di Risk Assessment, la Banca ha individuato le categorie di reato previste dal D.Lgs. 231/2001 ritenute astrattamente applicabili alla propria operatività, tenendo conto:

- delle attività svolte;
- della struttura organizzativa;
- dei processi aziendali;
- dei rapporti con clienti, fornitori, partner e Pubbliche Amministrazioni;
- delle modalità operative proprie del settore bancario e finanziario.

Per ciascuna categoria di reato rilevante sono state individuate:

- le attività sensibili;
- le funzioni aziendali coinvolte;
- i principali scenari di rischio;
- i presidi organizzativi, procedurali e di controllo adottati dalla Banca;
- il livello di rischio residuo risultante dall'attività di valutazione effettuata.

Le categorie di reato ritenute rilevanti per la Banca sono riportate nella matrice di Risk Assessment allegata al presente Modello.

Per le categorie di reato ritenute non applicabili o caratterizzate da rischio remoto, la Banca ha comunque effettuato una valutazione preliminare nell'ambito dell'attività di Risk Assessment, tenendo conto delle caratteristiche operative e organizzative aziendali.

Le attività sensibili e i relativi presidi di controllo sono oggetto di aggiornamento periodico in funzione:

- dell'evoluzione normativa;
- delle modifiche organizzative e operative della Banca;
- delle risultanze delle attività di controllo;
- delle verifiche svolte dall'Organismo di Vigilanza;
- dell'evoluzione dei rischi aziendali e dei presidi di mitigazione adottati.

3.1 Reati a rischiosità inerente rilevante

Rientrano nella presente categoria le fattispecie di reato che, in considerazione dell'operatività della Banca, delle attività svolte e delle caratteristiche del settore bancario e finanziario, presentano un livello di esposizione al rischio significativo e richiedono pertanto specifici presidi organizzativi, procedurali e di controllo.

3.1.1 Reati commessi nei rapporti con la Pubblica Amministrazione

La presente sezione si riferisce ai reati previsti dagli artt. 24 e 25 del D.Lgs. 231/2001, relativi ai rapporti con la Pubblica Amministrazione.

Ai fini del presente Modello, assumono particolare rilevanza, tra gli altri:

- corruzione;
- induzione indebita a dare o promettere utilità;
- concussione;
- truffa ai danni dello Stato o di ente pubblico;
- indebita percezione di erogazioni pubbliche;
- frode informatica ai danni dello Stato o di ente pubblico;
- traffico di influenze illecite.

Attività sensibili

Le principali attività sensibili individuate dalla Banca riguardano:

- gestione dei rapporti con Autorità di Vigilanza e Pubbliche Autorità;
- gestione di ispezioni, verifiche e accertamenti;
- partecipazione a bandi, finanziamenti o contributi pubblici;
- gestione degli adempimenti regolamentari e delle segnalazioni di vigilanza;
- gestione dei rapporti con consulenti, fornitori e soggetti terzi operanti per conto della Banca;
- gestione delle spese di rappresentanza, omaggi e liberalità;
- gestione del contenzioso e dei rapporti con l'Autorità Giudiziaria;
- processi autorizzativi e rapporti istituzionali.

Funzioni coinvolte

Le attività sensibili possono coinvolgere, a diverso titolo:

- Consiglio di Amministrazione;
- Direzione Generale;
- Funzioni Compliance e Antiriciclaggio
- Funzione Risk Management;
- Internal Audit;
- Funzione Contabilità, Segnalazioni e Bilancio;
- Funzione Commerciale;
- Risorse Umane;
- Funzione Organizzazione e ICT;
- ogni altra funzione che intrattenga rapporti con soggetti pubblici o incaricati di pubblico servizio.

Principi generali di comportamento

Nello svolgimento delle attività sensibili è fatto obbligo di:

- operare nel rispetto della normativa vigente e delle procedure aziendali;
- mantenere comportamenti improntati a correttezza, trasparenza e tracciabilità;
- garantire la completezza e veridicità delle informazioni trasmesse alla Pubblica Amministrazione;
- assicurare la segregazione dei compiti e la tracciabilità dei processi autorizzativi;
- documentare i rapporti intrattenuti con esponenti della Pubblica Amministrazione;
- segnalare tempestivamente eventuali anomalie o richieste non conformi alla normativa.

È fatto divieto di:

- promettere, offrire o corrispondere denaro, utilità o vantaggi indebiti a pubblici ufficiali o incaricati di pubblico servizio;
- alterare dati, informazioni o documentazione destinata alla Pubblica Amministrazione;
- porre in essere comportamenti finalizzati a ottenere indebiti vantaggi o agevolazioni;
- utilizzare consulenti, intermediari o terzi per finalità illecite o non trasparenti;
- ostacolare attività ispettive o di vigilanza.

Presidi di controllo

La Banca adotta specifici presidi organizzativi e di controllo, tra cui:

- sistema formalizzato di deleghe e poteri;
- segregazione dei compiti;
- procedure interne e controlli autorizzativi;
- tracciabilità delle operazioni e dei flussi documentali;
- controlli di secondo livello delle funzioni competenti;
- monitoraggio dei rapporti con la Pubblica Amministrazione;
- attività di formazione del personale;
- flussi informativi verso l'Organismo di Vigilanza.

3.1.2 Delitti informatici e trattamento illecito dei dati

La presente sezione si riferisce ai reati previsti dall'art. 24-bis del D.Lgs. 231/2001, relativi ai delitti informatici e al trattamento illecito dei dati.

Ai fini del presente Modello assumono particolare rilevanza, tra gli altri:

- accesso abusivo a sistemi informatici o telematici;
- detenzione e diffusione abusiva di codici di accesso;
- diffusione di programmi diretti a danneggiare o interrompere sistemi informatici;
- danneggiamento di sistemi informatici o dati;
- intercettazione illecita di comunicazioni informatiche;
- falsità in documenti informatici;
- violazioni in materia di sicurezza informatica e protezione dei dati.

In considerazione della natura dell'attività bancaria svolta, della rilevanza dei sistemi ICT e della gestione di dati e informazioni riferibili alla clientela, tali fattispecie assumono particolare rilevanza nell'ambito del sistema dei controlli interni della Banca.

Attività sensibili

Le principali attività sensibili individuate riguardano:

- gestione dei sistemi informatici e delle infrastrutture ICT;
- gestione degli accessi logici e delle credenziali;
- utilizzo degli applicativi bancari e dei sistemi di pagamento;
- gestione dei dati della clientela e delle informazioni riservate;
- gestione della sicurezza informatica e della continuità operativa;
- gestione dei rapporti con fornitori ICT e outsourcer;
- utilizzo della posta elettronica e degli strumenti informatici aziendali;
- gestione degli incidenti di sicurezza informatica;

- conservazione, archiviazione e protezione dei dati.

Funzioni coinvolte

Le attività sensibili possono coinvolgere, a diverso titolo:

- Funzione Organizzazione e IT;
- Funzione Compliance e Antiriciclaggio;
- Funzione Risk Management;
- Internal Audit;
- tutte le funzioni aziendali che utilizzano sistemi informatici e trattano dati aziendali o della clientela;
- fornitori e outsourcer ICT.

Principi generali di comportamento

Nello svolgimento delle attività sensibili è fatto obbligo di:

- utilizzare sistemi, dati e applicativi aziendali esclusivamente per finalità lavorative autorizzate;
- operare nel rispetto delle procedure aziendali in materia di sicurezza informatica e protezione dei dati;
- garantire la riservatezza, integrità e disponibilità delle informazioni;
- custodire correttamente credenziali e strumenti di autenticazione;
- segnalare tempestivamente anomalie, incidenti informatici o accessi non autorizzati;
- assicurare la tracciabilità delle operazioni effettuate sui sistemi aziendali.

È fatto divieto di:

- accedere abusivamente a sistemi informatici o dati aziendali;
- acquisire, consultare o utilizzare dati della clientela in assenza di autorizzazione;
- alterare, distruggere o diffondere abusivamente dati o informazioni aziendali;
- condividere credenziali di accesso o eludere i sistemi di sicurezza;
- installare software o strumenti non autorizzati;
- utilizzare strumenti informatici aziendali per finalità illecite o non connesse all'attività lavorativa.

Presidi di controllo

La Banca adotta specifici presidi organizzativi e di controllo, tra cui:

- policy e procedure in materia di sicurezza informatica;
- sistemi di autenticazione e profilazione degli accessi;
- segregazione dei privilegi autorizzativi;
- sistemi di monitoraggio e logging degli accessi;
- controlli sugli accessi ai dati della clientela;
- sistemi di backup e disaster recovery;
- gestione degli incidenti ICT e continuità operativa;
- controlli sui fornitori e outsourcer ICT;
- attività di formazione e sensibilizzazione del personale;
- flussi informativi verso le funzioni di controllo e l'Organismo di Vigilanza.

3.1.3 Reati societari

La presente sezione si riferisce ai reati previsti dall'art. 25-ter del D.Lgs. 231/2001, relativi ai reati societari.

Ai fini del presente Modello assumono particolare rilevanza, tra gli altri:

- false comunicazioni sociali;
- impedito controllo;
- indebita restituzione dei conferimenti;
- illecita influenza sull'assemblea;
- aggiotaggio;
- ostacolo all'esercizio delle funzioni delle Autorità pubbliche di vigilanza;
- corruzione tra privati.

In considerazione della natura dell'attività bancaria svolta, tali fattispecie assumono particolare rilievo con riferimento ai processi amministrativi, contabili, di reporting e di governo societario.

Attività sensibili

Le principali attività sensibili individuate riguardano:

- predisposizione del bilancio e delle comunicazioni sociali;
- gestione della contabilità generale e delle registrazioni contabili;
- predisposizione delle segnalazioni di vigilanza;
- gestione dei rapporti con Autorità di Vigilanza, revisori e organi sociali;
- gestione delle operazioni societarie e straordinarie;
- gestione dei flussi informativi verso il Consiglio di Amministrazione e il Collegio Sindacale;
- gestione dei conflitti di interesse;
- gestione dei rapporti con fornitori, consulenti e partner commerciali;
- gestione delle informazioni privilegiate e delle comunicazioni al mercato.

Funzioni coinvolte

Le attività sensibili possono coinvolgere, a diverso titolo:

- Consiglio di Amministrazione;
- Collegio Sindacale;
- Direzione Generale;
- Funzione Contabilità, Segnalazioni e Bilancio;
- Funzione Compliance e Antiriciclaggio;
- Funzione Risk Management;
- Internal Audit;
- Funzione Legale;
- tutte le funzioni coinvolte nella formazione dei dati contabili e societari.

Principi generali di comportamento

Nello svolgimento delle attività sensibili è fatto obbligo di:

- garantire correttezza, completezza, accuratezza e trasparenza delle informazioni contabili e societarie;
- assicurare la tracciabilità delle operazioni e dei processi autorizzativi;
- rispettare le procedure aziendali e i poteri attribuiti;

- collaborare con gli organi sociali, le Autorità di Vigilanza e i revisori;
- assicurare la corretta conservazione della documentazione societaria e contabile;
- segnalare tempestivamente eventuali anomalie o situazioni di conflitto di interesse.

È fatto divieto di:

- rappresentare fatti non rispondenti al vero o omettere informazioni rilevanti nelle comunicazioni sociali;
- ostacolare le attività di controllo o vigilanza;
- alterare dati, informazioni o documentazione contabile;
- utilizzare informazioni riservate per finalità indebite;
- porre in essere comportamenti suscettibili di compromettere la correttezza e trasparenza della gestione societaria.

Presidi di controllo

La Banca adotta specifici presidi organizzativi e di controllo, tra cui:

- procedure amministrativo-contabili formalizzate;
- segregazione dei compiti e sistemi autorizzativi;
- controlli di linea e di secondo livello;
- verifiche sulla correttezza delle registrazioni contabili;
- controlli sui flussi informativi verso organi sociali e Autorità di Vigilanza;
- sistemi di tracciabilità documentale;
- monitoraggio dei conflitti di interesse;
- attività di formazione del personale;
- flussi informativi verso l'Organismo di Vigilanza.

3.1.4 Reati di riciclaggio, autoriciclaggio e finanziamento del terrorismo

La presente sezione si riferisce ai reati previsti dall'art. 25-octies del D.Lgs. 231/2001, nonché ai delitti connessi al finanziamento del terrorismo, con particolare riferimento alle fattispecie di:

- ricettazione;
- riciclaggio;
- impiego di denaro, beni o utilità di provenienza illecita;
- autoriciclaggio.

In considerazione dell'attività svolta dalla Banca e della rilevanza dei presidi antiriciclaggio nel settore bancario e finanziario, tali fattispecie assumono particolare rilevanza nell'ambito del presente Modello.

Attività sensibili

Le principali attività sensibili individuate riguardano:

- instaurazione e gestione dei rapporti continuativi con la clientela;
- attività di adeguata verifica e identificazione della clientela;
- gestione dell'operatività bancaria e finanziaria;
- esecuzione di bonifici, trasferimenti di fondi e operazioni di pagamento;
- gestione di operazioni con controparti estere;
- monitoraggio delle operazioni anomale;
- gestione delle Segnalazioni di Operazioni Sospette (SOS);

- gestione dei rapporti con soggetti ad alto profilo di rischio;
- concessione del credito e gestione delle garanzie;
- utilizzo di contante e strumenti di pagamento.

Funzioni coinvolte

Le attività sensibili possono coinvolgere, a diverso titolo:

- Funzione Commerciale;
- Funzione Compliance e Antiriciclaggio;
- Funzione Crediti;
- Funzione Operations, Tesoreria e Estero;
- Funzione Risk Management;
- Internal Audit;
- Funzione Organizzazione e IT;
- tutte le strutture coinvolte nella gestione dei rapporti con la clientela e dei flussi finanziari.

Principi generali di comportamento

Nello svolgimento delle attività sensibili è fatto obbligo di:

- operare nel rispetto della normativa antiriciclaggio e delle procedure aziendali;
- assicurare adeguata conoscenza della clientela, del titolare effettivo e della finalità delle operazioni;
- verificare la coerenza delle operazioni rispetto al profilo economico-finanziario del cliente;
- monitorare eventuali anomalie operative;
- garantire la tracciabilità delle operazioni e dei controlli effettuati;
- collaborare con le funzioni di controllo e con le Autorità competenti.

È fatto divieto di:

- instaurare o mantenere rapporti in assenza dei presidi previsti dalla normativa AML/CFT;
- agevolare operazioni finalizzate al riciclaggio o all'occultamento di fondi di provenienza illecita;
- omettere controlli o verifiche obbligatorie;
- alterare dati o informazioni relativi alla clientela o alle operazioni effettuate;
- frazionare artificiosamente operazioni o utilizzare strumenti finalizzati ad eludere la normativa vigente.

Presidi di controllo

La Banca adotta specifici presidi organizzativi e di controllo, tra cui:

- sistema dei controlli antiriciclaggio;
- procedure di adeguata verifica della clientela;
- sistemi di monitoraggio delle operazioni;
- profilazione della clientela e valutazione del rischio AML;
- controlli sulle operazioni anomale e gestione delle SOS;
- controlli su liste e misure restrittive;
- segregazione dei compiti e sistemi autorizzativi;
- controlli di secondo livello della Funzione Antiriciclaggio;
- attività di formazione specialistica del personale;
- flussi informativi verso le funzioni di controllo e l'Organismo di Vigilanza.

3.1.5 Reati tributari

La presente sezione si riferisce ai reati previsti dall'art. 25-quinquiesdecies del D.Lgs. 231/2001, relativi ai reati tributari.

Ai fini del presente Modello assumono particolare rilevanza, tra gli altri:

- dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti;
- dichiarazione fraudolenta mediante altri artifici;
- emissione di fatture o altri documenti per operazioni inesistenti;
- occultamento o distruzione di documenti contabili;
- sottrazione fraudolenta al pagamento delle imposte.

Tali fattispecie assumono rilievo principalmente con riferimento ai processi amministrativi, contabili, fiscali e di gestione dei rapporti con fornitori e consulenti.

Attività sensibili

Le principali attività sensibili individuate riguardano:

- gestione della contabilità generale;
- predisposizione delle dichiarazioni fiscali;
- gestione degli adempimenti tributari;
- registrazione delle operazioni contabili;
- gestione del ciclo passivo e dei rapporti con fornitori e consulenti;
- gestione della documentazione fiscale e amministrativa;
- gestione delle operazioni infragruppo e straordinarie;
- gestione dei rapporti con l'Amministrazione Finanziaria.

Funzioni coinvolte

Le attività sensibili possono coinvolgere, a diverso titolo:

- Funzione Contabilità, Segnalazioni e Bilancio;
- Funzione Compliance e Antiriciclaggio;
- Direzione Generale;
- Funzione Organizzazione e IT;
- Internal Audit;
- consulenti fiscali e professionisti esterni eventualmente incaricati dalla Banca.

Principi generali di comportamento

Nello svolgimento delle attività sensibili è fatto obbligo di:

- garantire correttezza, completezza e veridicità delle registrazioni contabili e fiscali;
- assicurare la tracciabilità delle operazioni e della documentazione di supporto;
- operare nel rispetto della normativa tributaria e delle procedure aziendali;
- verificare la coerenza e legittimità delle operazioni registrate;
- conservare correttamente la documentazione amministrativa e fiscale;
- collaborare con le funzioni di controllo e con le Autorità competenti.

È fatto divieto di:

- registrare operazioni inesistenti o non correttamente documentate;
- alterare o distruggere documentazione contabile o fiscale;
- predisporre dichiarazioni fiscali non veritiere;

- utilizzare documentazione falsa o incompleta;
- porre in essere comportamenti finalizzati all'evasione o all'elusione fraudolenta degli obblighi tributari.

Presidi di controllo

La Banca adotta specifici presidi organizzativi e di controllo, tra cui:

- procedure amministrativo-contabili formalizzate;
- segregazione dei compiti nei processi contabili e fiscali;
- controlli autorizzativi e di coerenza sulle registrazioni contabili;
- verifiche sulla documentazione fiscale e amministrativa;
- controlli di secondo livello delle funzioni competenti;
- tracciabilità delle operazioni e archiviazione documentale;
- monitoraggio dei rapporti con consulenti e fornitori;
- attività di formazione del personale;
- flussi informativi verso l'Organismo di Vigilanza.

3.1.6 Reati in materia di strumenti di pagamento diversi dai contanti

La presente sezione si riferisce ai reati previsti dall'art. 25-octies.1 del D.Lgs. 231/2001, relativi ai delitti in materia di strumenti di pagamento diversi dai contanti.

Ai fini del presente Modello assumono particolare rilevanza le fattispecie connesse all'utilizzo illecito, falsificazione, alterazione o indebita utilizzazione di strumenti di pagamento elettronici e mezzi di pagamento diversi dal contante.

In considerazione dell'operatività bancaria svolta, tali fattispecie assumono rilievo con riferimento ai servizi di pagamento, agli strumenti elettronici e ai canali digitali messi a disposizione della clientela.

Attività sensibili

Le principali attività sensibili individuate riguardano:

- emissione e gestione di carte di pagamento;
- gestione dei servizi di internet banking e mobile banking;
- gestione degli strumenti di pagamento elettronici;
- esecuzione di bonifici e operazioni di pagamento;
- gestione delle credenziali di autenticazione;
- gestione delle frodi informatiche e dei tentativi di utilizzo illecito degli strumenti di pagamento;
- monitoraggio delle operazioni anomale;
- gestione dei rapporti con provider di servizi di pagamento e outsourcer tecnologici.

Funzioni coinvolte

Le attività sensibili possono coinvolgere, a diverso titolo:

- Funzioni Operations, Tesoreria e estero;
- Funzione Organizzazione e IT;
- Funzione Compliance e Antiriciclaggio;
- Funzione Risk Management;
- Funzione Commerciale;
- Internal Audit;
- fornitori e outsourcer coinvolti nella gestione dei sistemi di pagamento.

Principi generali di comportamento

Nello svolgimento delle attività sensibili è fatto obbligo di:

- operare nel rispetto della normativa vigente e delle procedure aziendali;
- garantire la sicurezza e tracciabilità delle operazioni di pagamento;
- verificare la correttezza e coerenza delle operazioni effettuate;
- adottare adeguate misure di protezione delle credenziali e dei dati della clientela;
- segnalare tempestivamente anomalie, tentativi di frode o utilizzi non autorizzati degli strumenti di pagamento;
- collaborare con le funzioni di controllo e sicurezza informatica.

È fatto divieto di:

- utilizzare impropriamente strumenti di pagamento o credenziali di accesso;
- alterare o manipolare dati relativi alle operazioni di pagamento;
- eludere i sistemi di sicurezza e autenticazione;
- porre in essere comportamenti idonei a favorire frodi o utilizzi illeciti degli strumenti di pagamento.

Presidi di controllo

La Banca adotta specifici presidi organizzativi e di controllo, tra cui:

- sistemi di autenticazione forte e profilazione degli accessi;
- monitoraggio delle operazioni di pagamento;
- sistemi antifrode;
- controlli sui canali digitali e sui servizi di pagamento;
- segregazione dei compiti e controlli autorizzativi;
- monitoraggio degli accessi ai sistemi;
- gestione degli incidenti informatici e delle frodi;
- attività di formazione e sensibilizzazione del personale;
- flussi informativi verso le funzioni di controllo e l'Organismo di Vigilanza.

3.1.7 Delitti di criminalità organizzata

La presente sezione si riferisce ai reati previsti dall'art. 24-ter del D.Lgs. 231/2001, relativi ai delitti di criminalità organizzata.

Ai fini del presente Modello assumono particolare rilevanza le fattispecie che possono astrattamente manifestarsi nell'ambito dell'operatività bancaria e finanziaria, anche con riferimento ai rischi di infiltrazione criminale, utilizzo illecito dei rapporti bancari, utilizzo di società schermate o interposizioni fittizie.

Attività sensibili

Le principali attività sensibili individuate riguardano:

- instaurazione e gestione dei rapporti con la clientela;
- attività di adeguata verifica della clientela;
- gestione dell'operatività finanziaria e dei flussi di pagamento;
- gestione di operazioni con controparti estere;
- affidamenti e concessione del credito;

- gestione dei rapporti con fornitori, consulenti e partner commerciali;
- gestione delle operazioni potenzialmente anomale ai fini antiriciclaggio;
- gestione dei rapporti con soggetti politicamente esposti o ad alto profilo di rischio;
- attività di esternalizzazione e rapporti con outsourcer.

Funzioni coinvolte

Le attività sensibili possono coinvolgere, a diverso titolo:

- Funzione Commerciale;
- Funzione Compliance e Antiriciclaggio;
- Funzione Risk Management;
- Funzione Crediti;
- Funzione Operations, Tesoreria e Estero;
- Internal Audit;
- Funzione Legale;
- tutte le strutture coinvolte nei rapporti con clientela, fornitori e controparti.

Principi generali di comportamento

Nello svolgimento delle attività sensibili è fatto obbligo di:

- operare nel rispetto della normativa vigente e delle procedure aziendali;
- assicurare adeguata conoscenza della clientela e delle controparti;
- verificare la coerenza economica e finanziaria delle operazioni effettuate;
- monitorare eventuali anomalie operative o comportamenti non coerenti con il profilo del cliente;
- garantire la tracciabilità delle operazioni e dei processi decisionali;
- collaborare con le funzioni di controllo competenti.

È fatto divieto di:

- instaurare o mantenere rapporti con soggetti coinvolti in attività criminose o privi dei necessari requisiti di trasparenza;
- agevolare operazioni finalizzate al riciclaggio, all'occultamento di fondi illeciti o al finanziamento di attività criminali;
- omettere controlli o verifiche previsti dalla normativa interna o esterna;
- alterare informazioni o documentazione relativa alla clientela o alle operazioni effettuate;
- porre in essere comportamenti idonei ad agevolare organizzazioni criminali.

Presidi di controllo

La Banca adotta specifici presidi organizzativi e di controllo, tra cui:

- procedure di adeguata verifica della clientela;
- sistemi di monitoraggio delle operazioni;
- controlli antiriciclaggio e presidi AML/CFT;
- sistemi di profilazione della clientela;
- controlli sui rapporti con fornitori e partner;
- segregazione dei compiti e controlli autorizzativi;
- attività di controllo di secondo livello;
- formazione del personale sui rischi di criminalità finanziaria;
- flussi informativi verso le funzioni di controllo e l'Organismo di Vigilanza.

3.1.8 Reati in materia di violazione delle misure restrittive dell'Unione Europea

La presente sezione si riferisce ai reati previsti dall'art. 25-octies.2 del D.Lgs. 231/2001.

In considerazione dell'operatività internazionale della Banca, della presenza di clientela estera e della gestione di operazioni finanziarie verso controparti nazionali ed estere, tali fattispecie presentano un livello di rischiosità inerente rilevante.

Attività sensibili

Le attività sensibili individuate riguardano principalmente:

- apertura e gestione dei rapporti continuativi;
- operatività con clientela estera;
- esecuzione di bonifici e trasferimenti internazionali;
- controlli AML e sanctions screening;
- gestione delle operazioni sospette;
- monitoraggio delle liste sanzionatorie e delle controparti.

Funzioni coinvolte

Le principali funzioni coinvolte sono:

- Funzione Compliance e Antiriciclaggio;
- Funzione Operations, Tesoreria e Estero;
- Funzione Commerciale;
- Funzione Crediti;
- Internal Audit;
- Funzione Organizzazione e IT.

Principi generali di comportamento

I destinatari del Modello sono tenuti a:

- operare nel rispetto della normativa nazionale ed europea in materia di sanzioni internazionali e misure restrittive;
- garantire correttezza, completezza e tracciabilità delle verifiche effettuate;
- astenersi dall'instaurare o mantenere rapporti con soggetti sottoposti a restrizioni o sanzioni;
- segnalare tempestivamente eventuali anomalie o operazioni sospette alle funzioni competenti;
- collaborare con le funzioni di controllo e con l'Organismo di Vigilanza.

Presidi di controllo

La Banca adotta specifici presidi organizzativi e procedurali finalizzati a:

- effettuare controlli sulle liste sanzionatorie nazionali e internazionali;
- verificare controparti e titolari effettivi;
- monitorare operazioni e flussi finanziari internazionali;
- assicurare la tracciabilità delle verifiche svolte;
- disciplinare escalation e blocco delle operazioni anomale;
- garantire adeguati flussi informativi verso le funzioni di controllo.

3.2 Reati a rischiosità inerente moderata

Rientrano nella presente categoria le fattispecie di reato che, pur risultando astrattamente applicabili all'operatività della Banca, presentano un livello di esposizione al rischio non elevato in relazione alle caratteristiche dei processi aziendali e delle attività svolte.

3.2.1 Reati in materia di salute e sicurezza sul lavoro

La presente sezione si riferisce ai reati previsti dall'art. 25-septies del D.Lgs. 231/2001, relativi ai delitti di omicidio colposo e lesioni personali colpose gravi o gravissime commessi con violazione delle norme in materia di salute e sicurezza sul lavoro.

La Banca riconosce la tutela della salute e sicurezza dei lavoratori quale principio fondamentale della propria attività, promuovendo condizioni di lavoro conformi alla normativa vigente e ai principi di prevenzione e protezione.

Attività sensibili

Le principali attività sensibili individuate riguardano:

- gestione degli ambienti di lavoro e delle sedi aziendali;
- valutazione dei rischi e aggiornamento del Documento di Valutazione dei Rischi (DVR);
- gestione delle misure di prevenzione e protezione;
- gestione della formazione del personale in materia di salute e sicurezza;
- gestione di appalti, fornitori e manutenzioni;
- gestione delle emergenze e della continuità operativa;
- utilizzo delle attrezzature di lavoro e dei dispositivi aziendali;
- gestione degli infortuni e degli eventi incidentali.

Funzioni coinvolte

Le attività sensibili possono coinvolgere, a diverso titolo:

- Datore di Lavoro;
- Direzione Generale;
- Responsabile del Servizio di Prevenzione e Protezione (RSPP);
- Risorse Umane;
- Funzione Organizzazione e IT;
- Funzione Compliance e Antiriciclaggio;
- Internal Audit;
- lavoratori, preposti, dirigenti e soggetti terzi operanti presso le sedi della Banca.

Principi generali di comportamento

Nello svolgimento delle attività sensibili è fatto obbligo di:

- operare nel rispetto della normativa vigente in materia di salute e sicurezza sul lavoro;
- adottare comportamenti improntati alla prevenzione dei rischi;
- rispettare le procedure aziendali e le misure di sicurezza adottate dalla Banca;
- partecipare alle attività di formazione e informazione previste;
- segnalare tempestivamente anomalie, situazioni di rischio o eventi incidentali;
- collaborare con le funzioni competenti nell'attuazione delle misure di prevenzione e protezione.

È fatto divieto di:

- porre in essere comportamenti che possano compromettere la salute e sicurezza dei lavoratori;

- eludere le misure di prevenzione e protezione adottate dalla Banca;
- omettere controlli o segnalazioni relative a situazioni di rischio;
- utilizzare attrezzature o dispositivi in modo non conforme alle disposizioni aziendali.

Presidi di controllo

La Banca adotta specifici presidi organizzativi e di controllo, tra cui:

- sistema di gestione della salute e sicurezza sul lavoro;
- Documento di Valutazione dei Rischi (DVR);
- procedure e misure di prevenzione e protezione;
- monitoraggio degli ambienti di lavoro;
- attività di formazione e informazione del personale;
- gestione degli appalti e dei fornitori;
- controlli periodici e verifiche ispettive;
- gestione degli eventi incidentali e delle azioni correttive;
- flussi informativi verso le funzioni competenti e l'Organismo di Vigilanza.

3.2.2 Reati di contrabbando

La presente sezione si riferisce ai reati previsti dall'art. 25-sexiesdecies del D.Lgs. 231/2001, relativi ai reati di contrabbando.

Pur non svolgendo attività direttamente connesse all'importazione o commercializzazione di merci, la Banca ritiene opportuno presidiare i rischi indirettamente connessi a operazioni finanziarie, rapporti con controparti estere e movimentazioni di fondi potenzialmente collegabili a fenomeni di contrabbando o traffici illeciti.

Attività sensibili

Le principali attività sensibili individuate riguardano:

- gestione di operazioni finanziarie con controparti estere;
- esecuzione di pagamenti internazionali e trasferimenti di fondi;
- attività di trade finance e operazioni connesse al commercio internazionale;
- gestione dei rapporti con clienti operanti in settori a rischio;
- monitoraggio delle operazioni anomale;
- gestione dei controlli antiriciclaggio e delle misure restrittive internazionali.

Funzioni coinvolte

Le attività sensibili possono coinvolgere, a diverso titolo:

- Funzione Commerciale;
- Funzione Operations, Tesoreria e Estero;
- Funzione Compliance e Antiriciclaggio;
- Funzione Risk Management;
- Internal Audit;
- funzioni coinvolte nella gestione di operazioni internazionali e dei flussi finanziari.

Principi generali di comportamento

Nello svolgimento delle attività sensibili è fatto obbligo di:

- operare nel rispetto della normativa vigente e delle procedure aziendali;
- assicurare adeguata conoscenza della clientela e delle controparti;
- verificare la coerenza economica e finanziaria delle operazioni effettuate;
- monitorare eventuali anomalie operative o transazioni non coerenti con il profilo del cliente;
- collaborare con le funzioni di controllo competenti;
- garantire la tracciabilità delle operazioni effettuate.

È fatto divieto di:

- agevolare operazioni connesse a traffici illeciti o fenomeni di contrabbando;
- omettere controlli o verifiche previsti dalla normativa interna o esterna;
- alterare dati, informazioni o documentazione relativi alle operazioni effettuate;
- porre in essere comportamenti finalizzati ad eludere controlli o misure restrittive.

Presidi di controllo

La Banca adotta specifici presidi organizzativi e di controllo, tra cui:

- procedure di adeguata verifica della clientela;
- sistemi di monitoraggio delle operazioni finanziarie;
- controlli AML/CFT e screening sulle controparti;
- controlli sulle operazioni internazionali;
- segregazione dei compiti e controlli autorizzativi;
- monitoraggio delle operazioni anomale;
- attività di formazione del personale;
- flussi informativi verso le funzioni di controllo e l'Organismo di Vigilanza.

3.2.3 Reati transnazionali

La presente sezione si riferisce ai reati transnazionali previsti dall'art. 10 della Legge 16 marzo 2006, n. 146.

Ai fini del presente Modello assumono rilievo le fattispecie di reato caratterizzate dal coinvolgimento di più Stati ovvero da attività criminali svolte in ambito internazionale, con particolare riferimento ai rischi connessi ai flussi finanziari transfrontalieri, ai rapporti con controparti estere e alla possibile agevolazione di attività illecite di natura internazionale.

Attività sensibili

Le principali attività sensibili individuate riguardano:

- gestione di operazioni finanziarie internazionali;
- trasferimenti transfrontalieri di fondi;
- rapporti con banche corrispondenti e controparti estere;
- gestione della clientela estera;
- operazioni con Paesi o settori ad alto rischio;
- attività di trade finance e servizi di pagamento internazionali;
- gestione delle misure restrittive e dei controlli internazionali;
- monitoraggio delle operazioni anomale e delle transazioni sospette.

Funzioni coinvolte

Le attività sensibili possono coinvolgere, a diverso titolo:

- Funzione Commerciale;
- Funzione Operations, Tesoreria e Estero;
- Funzione Compliance e Antiriciclaggio;
- Funzione Risk Management;
- Internal Audit;
- Funzione Legale;
- strutture coinvolte nella gestione dei rapporti internazionali e dei flussi finanziari.

Principi generali di comportamento

Nello svolgimento delle attività sensibili è fatto obbligo di:

- operare nel rispetto della normativa nazionale e internazionale applicabile;
- assicurare adeguata conoscenza della clientela e delle controparti estere;
- monitorare la coerenza economica e finanziaria delle operazioni internazionali;
- verificare eventuali anomalie operative o profili di rischio elevato;
- rispettare le misure restrittive e i controlli previsti dalla normativa vigente;
- garantire la tracciabilità delle operazioni e dei controlli effettuati.

È fatto divieto di:

- agevolare attività criminose di natura transnazionale;
- instaurare rapporti con soggetti o controparti sottoposti a restrizioni o sanzioni;
- omettere controlli o verifiche obbligatorie;
- alterare dati, informazioni o documentazione relativi alle operazioni effettuate;
- porre in essere comportamenti finalizzati ad eludere la normativa applicabile o i controlli previsti.

Presidi di controllo

La Banca adotta specifici presidi organizzativi e di controllo, tra cui:

- procedure di adeguata verifica della clientela;
- sistemi di monitoraggio delle operazioni internazionali;
- controlli AML/CFT e screening sulle controparti;
- controlli sulle misure restrittive internazionali;
- segregazione dei compiti e controlli autorizzativi;
- monitoraggio delle operazioni anomale;
- attività di formazione specialistica del personale;
- flussi informativi verso le funzioni di controllo e l'Organismo di Vigilanza.

3.2.4 Reati in materia di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare

La presente sezione si riferisce ai reati previsti dall'art. 25-duodecies del D.Lgs. 231/2001, relativi all'impiego di cittadini di Paesi terzi il cui soggiorno è irregolare, nonché alle fattispecie connesse al favoreggiamento dell'immigrazione clandestina.

Tali fattispecie assumono rilievo principalmente con riferimento ai processi di selezione, assunzione e gestione del personale, nonché ai rapporti con fornitori, consulenti e società appaltatrici.

Attività sensibili

Le principali attività sensibili individuate riguardano:

- selezione e assunzione del personale;
- gestione amministrativa dei rapporti di lavoro;
- verifica della documentazione relativa al soggiorno e alla permanenza sul territorio nazionale;
- gestione dei rapporti con società esterne, appaltatori e fornitori;
- affidamento di servizi in outsourcing;
- gestione degli accessi presso sedi e strutture aziendali.

Funzioni coinvolte

Le attività sensibili possono coinvolgere, a diverso titolo:

- Risorse Umane;
- Funzione Organizzazione e IT;
- Funzione Compliance e Antiriciclaggio;
- Internal Audit;
- funzioni aziendali che gestiscono rapporti con fornitori e personale esterno.

Principi generali di comportamento

Nello svolgimento delle attività sensibili è fatto obbligo di:

- operare nel rispetto della normativa vigente in materia di lavoro e immigrazione;
- verificare preventivamente la regolarità della documentazione relativa ai lavoratori;
- monitorare la permanenza dei requisiti previsti dalla normativa;
- assicurare la corretta gestione documentale e la tracciabilità dei controlli effettuati;
- verificare l'affidabilità dei fornitori e degli appaltatori.

È fatto divieto di:

- instaurare rapporti di lavoro in assenza dei requisiti previsti dalla normativa vigente;
- omettere controlli o verifiche documentali obbligatorie;
- utilizzare fornitori o appaltatori privi dei necessari requisiti di regolarità;
- alterare o falsificare documentazione relativa ai rapporti di lavoro o ai titoli di soggiorno.

Presidi di controllo

La Banca adotta specifici presidi organizzativi e di controllo, tra cui:

- procedure di selezione e assunzione del personale;
- controlli documentali sui titoli di soggiorno;
- verifiche periodiche sulla regolarità dei rapporti di lavoro;
- controlli sui fornitori e sugli appaltatori;
- segregazione dei compiti e controlli autorizzativi;
- tracciabilità della documentazione e delle verifiche effettuate;
- attività di formazione del personale;
- flussi informativi verso le funzioni di controllo e l'Organismo di Vigilanza.

3.2.5 Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità giudiziaria

La presente sezione si riferisce ai reati previsti dall'art. 25-decies del D.Lgs. 231/2001.

Tali fattispecie possono assumere rilievo principalmente nell'ambito della gestione del contenzioso, dei rapporti con l'Autorità Giudiziaria e delle attività ispettive o investigative e presentano un livello di rischiosità inerente moderata.

Attività sensibili

Le attività sensibili individuate riguardano principalmente:

- gestione del contenzioso civile, penale e amministrativo;
- rapporti con l'Autorità Giudiziaria;
- gestione delle richieste documentali e ispettive;
- rapporti con consulenti legali esterni;
- gestione delle attività di audit e verifica.

Funzioni coinvolte

Le principali funzioni coinvolte sono:

- Funzione Legale;
- Funzione Compliance e Antiriciclaggio;
- Internal Audit;
- Direzione Generale;
- Risorse Umane;
- Organismo di Vigilanza.

Principi generali di comportamento

I destinatari del Modello sono tenuti a:

- mantenere comportamenti improntati a correttezza, trasparenza e collaborazione con le Autorità;
- garantire veridicità, completezza e tracciabilità delle informazioni fornite;
- astenersi da qualsiasi comportamento volto a influenzare impropriamente soggetti chiamati a rendere dichiarazioni;
- collaborare con le funzioni di controllo e con l'Organismo di Vigilanza.

Presidi di controllo

La Banca adotta specifici presidi organizzativi e procedurali finalizzati a:

- disciplinare la gestione del contenzioso e dei rapporti con l'Autorità Giudiziaria;
- garantire segregazione dei ruoli e tracciabilità delle attività svolte;
- assicurare controlli sui flussi documentali e informativi;
- monitorare le attività affidate a consulenti e professionisti esterni;
- garantire adeguati flussi informativi verso l'Organismo di Vigilanza.

3.2.6 Delitti in materia di violazione del diritto d'autore

La presente sezione si riferisce ai reati previsti dall'art. 25-novies del D.Lgs. 231/2001.

Tali fattispecie possono assumere rilievo principalmente nell'ambito della gestione dei sistemi informativi, dell'utilizzo di software e strumenti digitali e della produzione di contenuti e documentazione aziendale, e presentano un livello di rischiosità inerente moderata.

Attività sensibili

Le attività sensibili individuate riguardano principalmente:

- acquisto, installazione e utilizzo di software e applicazioni informatiche;

- gestione e utilizzo di banche dati proprietarie o di terzi;
- utilizzo di contenuti digitali, documentazione e materiali protetti da diritti di proprietà intellettuale nell'ambito dell'attività operativa e commerciale;
- produzione e diffusione di materiali formativi, comunicativi e promozionali;
- gestione dei rapporti con fornitori di soluzioni informatiche e contenuti digitali.

Funzioni coinvolte

Le principali funzioni coinvolte sono:

- Funzione Organizzazione e IT;
- Funzione Compliance e Antiriciclaggio;
- Internal Audit;
- Responsabili di funzione per le rispettive dotazioni software.

Principi generali di comportamento

I destinatari del Modello sono tenuti a:

- utilizzare esclusivamente software e applicazioni regolarmente licenziati e autorizzati dalla Banca;
- astenersi dalla riproduzione, distribuzione o utilizzo non autorizzato di contenuti, documenti o materiali protetti da diritti di proprietà intellettuale;
- segnalare tempestivamente alla funzione competente qualsiasi utilizzo irregolare di software o contenuti digitali di cui vengano a conoscenza;
- rispettare i termini e le condizioni dei contratti di licenza stipulati dalla Banca con i fornitori di soluzioni informatiche;
- collaborare con le funzioni di controllo e con l'Organismo di Vigilanza.

Presidi di controllo

La Banca adotta specifici presidi organizzativi e procedurali finalizzati a:

- censire e monitorare il parco software installato, verificando la regolarità delle licenze e la conformità agli accordi contrattuali;
- disciplinare le modalità di acquisto e installazione di software attraverso procedure che prevedono autorizzazione preventiva della funzione IT;
- garantire la segregazione dei ruoli tra chi acquista, chi installa e chi utilizza i sistemi informatici;
- assicurare controlli periodici sull'utilizzo degli strumenti informatici aziendali, anche con riferimento all'accesso a contenuti protetti;
- monitorare i rapporti con i fornitori di soluzioni informatiche e contenuti digitali, verificando la conformità delle forniture agli accordi sottoscritti;
- garantire adeguati flussi informativi verso l'Organismo di Vigilanza.

3.2.7 Falsità in monete, carte di pubblico credito, valori di bollo e segni distintivi

La presente sezione si riferisce ai reati previsti dall'art. 25-bis del D.Lgs. 231/2001.

Tali fattispecie assumono rilievo principalmente nell'ambito della gestione del contante, delle operazioni di cassa e della verifica degli strumenti di pagamento in contante, e presentano un livello di rischiosità inerente moderata in considerazione dell'operatività bancaria svolta da Extrabanca, che include la gestione diretta di denaro contante e valori presso gli sportelli.

Attività sensibili

Le attività sensibili individuate riguardano principalmente:

- ricezione, controllo e gestione del denaro contante presso gli sportelli e le casse aziendali;
- verifica dell'autenticità delle banconote e monete ricevute dalla clientela;
- gestione e utilizzo di valori bollati, marche da bollo e altri valori di pubblico credito nell'ambito dell'operatività;
- operazioni di cambio valuta e gestione di valute estere;
- gestione dei versamenti e prelievi in contante da parte della clientela.

Funzioni coinvolte

Le principali funzioni coinvolte sono:

- Funzione Operations, Tesoreria e Estero;
- Area Commerciale;
- Funzione Compliance e Antiriciclaggio;
- Internal Audit.

Principi generali di comportamento

I destinatari del Modello sono tenuti a:

- applicare scrupolosamente le procedure di verifica dell'autenticità del denaro contante e degli altri valori ricevuti dalla clientela, avvalendosi degli strumenti tecnici messi a disposizione dalla Banca;
- segnalare immediatamente alla funzione competente e alle autorità previste dalla normativa vigente il ricevimento di banconote, monete o valori sospetti di falsità;
- astenersi dall'utilizzare, cedere o introdurre in circolazione valori di cui sia nota o sospettata la falsità;
- garantire la corretta custodia e gestione dei valori bollati e degli strumenti di pagamento in dotazione;
- collaborare con le funzioni di controllo e con l'Organismo di Vigilanza.

Presidi di controllo

La Banca adotta specifici presidi organizzativi e procedurali finalizzati a:

- dotare gli sportelli di strumenti tecnici per la verifica automatica dell'autenticità delle banconote, con aggiornamento periodico in conformità alle indicazioni della Banca d'Italia e della BCE;
- disciplinare le procedure operative di gestione del contante, con previsione di controlli sistematici su tutti i versamenti ricevuti dalla clientela;
- garantire la segregazione dei ruoli nelle operazioni di cassa, prevedendo controlli incrociati e quadratura giornaliera dei valori;
- assicurare la tracciabilità di tutte le operazioni di cassa e la conservazione della relativa documentazione;
- disciplinare le modalità di segnalazione e ritiro dalla circolazione delle banconote sospette, in conformità alla normativa Banca d'Italia;
- garantire adeguati flussi informativi verso l'Organismo di Vigilanza in caso di episodi rilevanti.

3.3 Reati a rischiosità inerente marginale

Rientrano nella presente categoria le fattispecie di reato che presentano profili di applicabilità limitati rispetto alle attività concretamente svolte dalla Banca e per le quali il rischio di commissione è ritenuto contenuto, anche in considerazione delle caratteristiche operative della Banca e dei presidi organizzativi e di controllo adottati.

Pur non costituendo aree di rischio primarie nell'ambito dell'operatività bancaria, tali fattispecie sono state oggetto di valutazione nell'ambito dell'attività di Risk Assessment ai fini della verifica della relativa applicabilità e dell'adeguatezza dei presidi di prevenzione esistenti.

3.3.1 Abusi di mercato

La presente sezione si riferisce ai reati previsti dall'art. 25-sexies del D.Lgs. 231/2001.

In considerazione dell'attività svolta dalla Banca, dell'assenza di attività di wealth management, investment banking o trading proprietario significativo, il rischio di commissione dei reati di abuso di mercato risulta limitato e principalmente connesso alla gestione del portafoglio titoli di proprietà e all'eventuale accesso a informazioni riservate o privilegiate.

La Banca adotta presidi organizzativi e procedurali finalizzati ad assicurare:

- la corretta gestione delle operazioni su strumenti finanziari;
- la riservatezza delle informazioni sensibili o privilegiate;
- la tracciabilità delle operazioni effettuate;
- il monitoraggio di eventuali conflitti di interesse;
- il rispetto della normativa applicabile in materia di abusi di mercato.

3.3.2 Reati ambientali

La presente sezione si riferisce ai reati previsti dall'art. 25-undecies del D.Lgs. 231/2001.

In considerazione dell'attività svolta dalla Banca, il rischio di commissione dei reati ambientali risulta limitato e principalmente connesso alla gestione degli immobili, dei rifiuti elettronici e delle attività affidate a fornitori e outsourcer.

La Banca adotta presidi organizzativi e procedurali finalizzati ad assicurare:

- il rispetto della normativa ambientale applicabile;
- la corretta gestione dei rifiuti e delle apparecchiature elettroniche;
- il monitoraggio dei fornitori incaricati di attività rilevanti sotto il profilo ambientale;
- la gestione degli immobili nel rispetto delle disposizioni vigenti.

3.3.3 Delitti contro l'industria e il commercio

La presente sezione si riferisce ai reati previsti dall'art. 25-bis.1 del D.Lgs. 231/2001.

In considerazione dell'attività bancaria svolta, tali fattispecie presentano profili di applicabilità limitati e prevalentemente indiretti, eventualmente connessi ai rapporti commerciali con fornitori, partner o soggetti terzi.

La Banca adotta presidi organizzativi e contrattuali finalizzati a garantire:

- correttezza e trasparenza nei rapporti commerciali;
- adeguata selezione e monitoraggio dei fornitori;
- rispetto della normativa applicabile in materia di concorrenza e proprietà industriale.

3.3.4 Reati di razzismo e xenofobia

La presente sezione si riferisce ai reati previsti dall'art. 25-terdecies del D.Lgs. 231/2001, che richiama l'art. 604-bis c.p. (propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica, nazionale o religiosa).

Tali fattispecie assumono per Extrabanca un rilievo specifico superiore alla media del settore bancario, in considerazione della natura e della vocazione della Banca, che opera prevalentemente a servizio di comunità di origine straniera e si avvale di personale multiculturale. Sebbene la condotta tipica richieda una componente di pubblicità o istigazione, che ne rende contenuta la probabilità di realizzazione, l'impatto reputazionale di qualsiasi contestazione in materia inciderebbe direttamente sul posizionamento identitario e commerciale della Banca in modo sproporzionato rispetto alla sua dimensione. Le fattispecie presentano pertanto un livello di rischiosità inerente marginale, superiore alla classificazione trascurabile applicabile a un istituto bancario generalista.

La Banca adotta presidi organizzativi e procedurali finalizzati a:

- garantire parità di trattamento a tutto il personale e a tutta la clientela, indipendentemente da nazionalità, etnia, religione o origine culturale;
- assicurare che i criteri di selezione del personale e di concessione dei servizi bancari siano oggettivi, documentati e non discriminatori;
- disciplinare la produzione e diffusione dei contenuti di comunicazione esterna, con verifica di conformità ai principi antidiscriminatori;
- prevedere percorsi di formazione periodica in materia di diversity e inclusione;
- garantire adeguati flussi informativi verso l'Organismo di Vigilanza.

3.4 Reati a rischiosità inerente trascurabile

Rientrano nella presente categoria le fattispecie di reato che, alla luce dell'attività di Risk Assessment svolta, risultano caratterizzate da un livello di esposizione remoto o trascurabile rispetto all'operatività, alla struttura organizzativa e alle attività concretamente svolte dalla Banca.

Tali categorie di reato sono state comunque considerate nell'ambito dell'attività di valutazione dei rischi ai fini della verifica della relativa applicabilità teorica.

3.4.1 Delitti con finalità di terrorismo o di eversione dell'ordine democratico

La presente sezione si riferisce ai reati previsti dall'art. 25-quater del D.Lgs. 231/2001.

In considerazione dell'attività svolta dalla Banca e dei presidi AML/CFT adottati, il rischio di commissione di tali reati è ritenuto trascurabile.

3.4.2 Pratiche di mutilazione degli organi genitali femminili

La presente sezione si riferisce ai reati previsti dall'art. 25-quater.1 del D.Lgs. 231/2001.

Tali fattispecie risultano non coerenti con l'operatività della Banca e presentano rischio trascurabile.

3.4.3 Delitti contro la personalità individuale

La presente sezione si riferisce ai reati previsti dall'art. 25-quinquies del D.Lgs. 231/2001.

In considerazione delle attività svolte dalla Banca e dell'assenza di processi operativi esposti a tali fattispecie, il rischio è ritenuto trascurabile.

3.4.4 Frode in competizioni sportive ed esercizio abusivo di giochi o scommesse

La presente sezione si riferisce ai reati previsti dall'art. 25-quaterdecies del D.Lgs. 231/2001.

Tali fattispecie risultano estranee alle attività caratteristiche svolte dalla Banca e presentano rischio trascurabile.

3.4.5 Delitti contro il patrimonio culturale

La presente sezione si riferisce ai reati previsti dall'art. 25-septiesdecies del D.Lgs. 231/2001.

Le fattispecie in esame risultano non coerenti con l'operatività bancaria svolta e presentano rischio trascurabile.

3.4.6 Riciclaggio, devastazione o saccheggio di beni culturali e paesaggistici

La presente sezione si riferisce ai reati previsti dall'art. 25-duodevicies del D.Lgs. 231/2001.

Alla luce dell'attività svolta dalla Banca e dei presidi AML adottati, il rischio associato a tali fattispecie è ritenuto trascurabile.

4. Aggiornamento della Parte Speciale

La presente Parte Speciale è oggetto di aggiornamento periodico in funzione:

- dell'evoluzione normativa;
- delle modifiche organizzative e operative della Banca;
- delle risultanze delle attività di Risk Assessment;
- degli esiti delle attività di controllo svolte dalle funzioni competenti e dall'Organismo di Vigilanza;
- dell'emersione di nuovi rischi o attività sensibili.

Le attività sensibili, i livelli di rischio, i presidi di controllo e i protocolli operativi adottati dalla Banca sono riportati nella documentazione di Risk Assessment e nei relativi allegati al presente Modello.

ALLEGATI

Allegato 1 – Risk Assessment

Il Risk Assessment contiene la mappatura delle attività sensibili, dei processi aziendali e delle funzioni coinvolte ai fini della prevenzione dei reati previsti dal D.Lgs. 231/2001.

Il documento riporta, per ciascuna categoria di reato rilevante, il livello di rischio inerente, i presidi di controllo adottati dalla Banca e la valutazione del rischio residuo.

Allegato 2 – Codice Etico

Il Codice Etico adottato da Extrabanca definisce i principi di comportamento, i valori e le regole etiche cui devono attenersi tutti i destinatari del Modello nello svolgimento delle rispettive attività.

Il Codice Etico costituisce parte integrante del Modello e rappresenta uno dei principali strumenti di prevenzione dei rischi di commissione dei reati previsti dal D.Lgs. 231/2001.

Allegato 3 – Regolamento dell'Organismo di Vigilanza

Il Regolamento dell'Organismo di Vigilanza disciplina composizione, funzionamento, poteri, responsabilità e modalità operative dell'OdV di Extrabanca.

Il Regolamento definisce inoltre i criteri di convocazione, verbalizzazione, reporting e gestione dei flussi informativi verso gli organi aziendali.

Allegato 4 – Flussi Informativi verso l'Organismo di Vigilanza

L'Allegato disciplina i flussi informativi periodici e ad evento verso l'Organismo di Vigilanza, individuando le informazioni rilevanti, le funzioni responsabili e le modalità di trasmissione.

I flussi informativi costituiscono uno strumento essenziale per consentire all'OdV lo svolgimento delle attività di vigilanza sull'efficace attuazione del Modello.

Allegato 5 – Organigramma Aziendale

L'Allegato riporta l'organigramma aziendale vigente di Extrabanca, con l'indicazione delle principali strutture organizzative, delle linee di riporto e delle funzioni aziendali coinvolte nei processi sensibili ai fini del D.Lgs. 231/2001.

L'organigramma costituisce elemento di riferimento per l'individuazione delle responsabilità e dei presidi organizzativi previsti dal Modello.

Allegato 6 – Normativa Interna Rilevante

L'Allegato 6 contiene l'elenco della principale normativa interna, delle policy, delle procedure e dei regolamenti aziendali rilevanti ai fini del Modello 231.

La normativa interna rappresenta parte integrante del sistema dei controlli della Banca e contribuisce alla prevenzione dei rischi di commissione dei reati-presupposto.

Allegato 7 – Codice Disciplinare Aziendale

L'Allegato contiene il sistema disciplinare adottato dalla Banca ai sensi del D.Lgs. 231/2001 e della normativa lavoristica applicabile.

Il Codice Disciplinare definisce le misure sanzionatorie applicabili in caso di violazione del Modello, del Codice Etico, delle procedure interne e delle disposizioni normative rilevanti.