



POLICY ANTIRICICLAGGIO

**Politica aziendale adottata ai sensi del D.Lgs. 231/07 e delle
“Disposizioni in materia di organizzazione, procedure e controlli
interni volti a prevenire l’utilizzo degli intermediari a fini di riciclaggio
e di finanziamento del terrorismo” emanate da Banca d’Italia**

POL102

Aggiornamento CdA 15/04/2026

Vers. 4.0

BANCA CAMBIANO 1884 S.p.A.

Sede legale e direzione generale: 50132 Firenze – Viale Antonio Gramsci, 34 – Tel. 0559768000 | Capitale sociale € 252.799.999,60 i.v. | Codice ABI 08425 | BIC CODE CRACIT33 | Sede operativa: 50051 Castelfiorentino (Fi) – Via Piave, 14 – Tel. 0559767000 | Iscritta all’Albo delle banche al n. 5667 | Codice fiscale, partita IVA e Numero di iscrizione nel Registro delle Imprese di Firenze 02599341209 | Aderente al Fondo Interbancario di Tutela dei Depositi, al Fondo Nazionale di Garanzia, al Conciliatore Bancario Finanziario, all’Arbitro Bancario Finanziario | Capogruppo del Gruppo Bancario Cambiano iscritto all’Albo dei Gruppi Bancari al n. 238 | e-mail: info@bancacambiano.it | PEC: pec@pec.bancacambiano.it | www.bancacambiano.it

Elenco versioni

Versione	Data
1.0	14/12/2015
2.0	02/01/2017
3.0	30/12/2019
3.1	27/02/2023
3.2	15/01/2025
3.3	12/03/2025
4.0	15/04/2026

INDICE

1	PREMESSA	5
1.1	FINALITA' DEL DOCUMENTO	5
1.2	CONTESTO NORMATIVO DI RIFERIMENTO	5
1.2.1	<i>Normativa esterna</i>	5
1.2.2	<i>Normativa interna</i>	7
1.3	DEFINIZIONI	8
2	ASSETTI DI GOVERNO, ORGANIZZAZIONE E CONTROLLI	14
2.1	SISTEMA ANTIRICICLAGGIO	14
2.2	ASSETTO DI GOVERNO	15
2.2.1	<i>Consiglio di Amministrazione</i>	15
2.2.2	<i>Direttore generale</i>	17
2.2.3	<i>Esponente responsabile per l'antiriciclaggio delle singole entita'</i>	18
2.2.4	<i>Esponente responsabile per l'antiriciclaggio di gruppo</i>	19
2.2.5	<i>Collegio Sindacale</i>	20
2.2.6	<i>Organismo di vigilanza ex D.Lgs. 231/01</i>	20
2.2.7	<i>Funzione Antiriciclaggio</i>	21
2.2.7.1	<i>Inquadramento, Criteri di selezione e Nomina del Responsabile della Funzione AML</i>	22
2.2.7.2	<i>Continuità operativa della funzione aml</i>	23
2.2.8	<i>Responsabile per le segnalazioni di operazioni sospette</i>	23
2.2.9	<i>Funzione di internal audit</i>	24
2.3	PRESIDIO DEL RISCHIO DI RICICLAGGIO NEL GRUPPO	24
2.3.1	<i>Integrazione nel presidio del rischio DI RICICLAGGIO</i>	24
2.3.2	<i>Esternalizzazione della Funzione Antiriciclaggio</i>	25
2.4	PRESIDIO SULL'APPLICAZIONE DELLE MISURE RESTRITTIVE	25
2.5	CONTROLLI INTERNI	26
2.5.1	<i>Profili strutturali</i>	26
2.5.2	<i>Coordinamento fra funzioni di controllo in materia AML</i>	28
2.5.3	<i>Sistema di whistleblowing</i>	28
3	ADEGUATA VERIFICA	29
3.1	NOZIONI CHIAVE SULL'ADEGUATA VERIFICA	29
3.1.1	<i>Approccio basato sul rischio</i>	29
3.1.2	<i>Obblighi di Adeguata Verifica</i>	29
3.1.3	<i>Operatività a distanza</i>	30
3.1.4	<i>Rapporti continuativi e operazioni occasionali</i>	31
3.2	PROFILATURA DELLA CLIENTELA	31
3.2.1	<i>Sistema di profilatura</i>	31
3.2.2	<i>Calibrazione delle misure di Adeguata Verifica in base al profilo di rischio</i>	31
3.2.3	<i>Aggiornamento del profilo di rischio</i>	32
3.3	GESTIONE DEI FATTORI DI RISCHIO	32
3.3.1	<i>Fattori di basso rischio</i>	33
3.3.1.1	<i>Fattori di basso rischio relativi al cliente, esecutore e titolare effettivo</i>	33
3.3.1.2	<i>Fattori di basso rischio relativi a prodotti, servizi, operazioni o canali di distribuzione</i>	33
3.3.1.3	<i>Fattori di basso rischio geografici</i>	34
3.3.2	<i>Fattori di rischio elevato</i>	34
3.3.2.1	<i>Fattori di rischio elevato relativi al cliente, esecutore e titolare effettivo</i>	34
3.3.2.2	<i>Fattori di rischio elevato relativi a prodotti, servizi, operazioni o canali di distribuzione</i>	36
3.3.2.3	<i>Fattori di rischio elevato geografici</i>	36
3.3.2.4	<i>Clienti indesiderati</i>	37
3.4	IDENTIFICAZIONE DEL TITOLARE EFFETTIVO	37
3.4.1	<i>Registro dei titolari effettivi</i>	38
3.5	CONTROLLO COSTANTE E TRANSACTION MONITORING	38
3.6	ADEGUATA VERIFICA ORDINARIA	39
3.7	ADEGUATA VERIFICA SEMPLIFICATA	39
3.8	ADEGUATA VERIFICA RAFFORZATA	40
3.9	PERSONE POLITICAMENTE ESPOSTE	41

3.10	RAPPORTI DI CORRISPONDENZA CON INTERMEDIARIO DI PAESE TERZO EXTRA UE.....	42
3.11	ASTENSIONE	42
3.12	DE-RISKING	43
3.13	ESECUZIONE DELL’ADEGUATA VERIFICA DA PARTE DI TERZI	43
3.14	ESECUZIONE DELL’ADEGUATA VERIFICA SUI FORNITORI.....	44
3.15	CONTROLLI IN MATERIA DI ANTITERRORISMO ED EMBARGHI INTERNAZIONALI E SUL TRASFERIMENTO DI FONDI	45
4	CONSERVAZIONE E SEGNALAZIONE.....	45
4.1	CONSERVAZIONE DEI DOCUMENTI E DEI DATI	45
4.1.1	<i>Conservazione dei documenti.....</i>	45
4.1.2	<i>Conservazione dei dati.....</i>	46
4.2	OBBLIGHI DI COMUNICAZIONE	46
4.2.1	<i>Flusso SARA.....</i>	46
4.2.2	<i>Comunicazioni oggettive</i>	46
5	PRESI SU PRODOTTI ASSICURATIVI, SERVIZI DI PAGAMENTO E STRUMENTI DIGITALI	47
5.1	PRESIDI SULLA DISTRIBUZIONE DI PRODOTTI ASSICURATIVI DA PARTE DELLA BANCA.....	47
5.2	PRESIDI IN MATERIA DI SERVIZI DI PAGAMENTO E DI STRUMENTI DIGITALI	48
6	AUTOVALUTAZIONE DEI RISCHI DI RICICLAGGIO E FINANZIAMENTO DEL TERRORISMO.....	48
7	FORMAZIONE	49
8	SANZIONI	50

1 PREMESSA

1.1 FINALITA' DEL DOCUMENTO

Il presente documento, rubricato *Policy Antiriciclaggio*, di seguito per brevità anche *Policy AML*, è adottato dalla Banca Cambiano 1884 Spa, di seguito per brevità *Banca*, per l'adeguamento alle previsioni delle *Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e di finanziamento del terrorismo*, di seguito per brevità anche *Disposizioni sull'organizzazione*, adottate con Provvedimento di Banca d'Italia del 23.03.2019, così come modificato dal Provvedimento del 1° agosto 2023, in attuazione dell'art. 7 del D.Lgs. 231/07 e s.m.i.

La presente *Policy AML* è adottata con delibera del Consiglio di amministrazione, su proposta del Direttore Generale, con parere favorevole del Collegio Sindacale.

La presente *Policy AML* delinea il sistema di prevenzione dei rischi connessi con il riciclaggio ed il finanziamento del terrorismo adottato dal Gruppo, tenuto conto delle dimensioni, delle specificità organizzative, dell'attività svolta e dei mercati in cui opera. In particolare, la *Policy AML* del Gruppo indica e motiva le scelte che il Gruppo in concreto intende compiere sui vari profili rilevanti in materia di assetti organizzativi, procedure e controlli interni, di adeguata verifica e di conservazione dei dati, in applicazione dell'approccio basato sul rischio (c.d. risk based approach) e, in particolare, delle risultanze dell'esercizio annuale di autovalutazione del livello di esposizione al rischio di riciclaggio. Le Società destinatarie applicano la *Policy AML* del Gruppo tenendo conto della natura, della dimensione e della complessità dell'attività svolta nonché della tipologia e della gamma dei servizi prestati.

Alla predisposizione della presente *Policy AML* ha concorso la Funzione Antiriciclaggio. La Funzione cura la diffusione della cultura dell'antiriciclaggio a tutto il personale, anche promuovendo la conoscenza e vigilando sull'applicazione della *Policy AML*.

1.2 CONTESTO NORMATIVO DI RIFERIMENTO

1.2.1 NORMATIVA ESTERNA

Di seguito si indicano i principali atti della normativa esterna rilevanti per l'inquadramento della presente *Policy*:

Normativa e regolamentazione dell'Unione Europea

- Direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio del 20 maggio 2015 relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo (per brevità "IV Direttiva");
- Regolamento (UE) 2015/847 del Parlamento europeo e del Consiglio del 20 maggio 2015 riguardante i dati informativi che accompagnano i trasferimenti di fondi (per brevità "Reg. 847");
- Regolamento delegato (UE) 2016 /1675, come tempo per tempo modificato e integrato, che integra la direttiva (UE) 2015/849/CE del Parlamento Europeo e del Consiglio per quanto concerne l'elenco dei Paesi terzi ad alto rischio;
- Direttiva (UE) 2018/843 del Parlamento europeo e del Consiglio del 30 maggio 2018 che modifica la Direttiva (UE) 2015/849 in materia di prevenzione del riciclaggio e del finanziamento del terrorismo (per brevità "V Direttiva");
- Regolamento (UE) 2023/1113 del Parlamento europeo e del Consiglio, del 31 maggio 2023, riguardante i dati informativi che accompagnano i trasferimenti di fondi e determinate cryptoattività e che modifica la direttiva (UE) 2015/849; - Regolamento (UE) 2024/886 del Parlamento europeo e

del Consiglio del 13 marzo 2024 che modifica i regolamenti (UE) n. 260/2012 e (UE) 2021/1230 e le direttive 98/26/CE e (UE) 2015/2366 per quanto riguarda i bonifici istantanei in euro;

- Regolamento (UE) 2024/1624 (AMLR) del Parlamento europeo e del Consiglio, del 31 maggio 2024, relativo alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo; decorrenza 10 luglio 2027 e sarà direttamente applicabile in ciascuno degli Stati membri, con l'obiettivo di armonizzare in modo esaustivo le norme antiriciclaggio in tutta l'Unione Europea;
- Orientamenti EBA (European Banking Authority) - GL/2021/02 - del 1° marzo 2021, ai sensi dell'articolo 17 e dell'articolo 18, paragrafo 4, della direttiva (UE) 2015/849 sulle misure di adeguata verifica della clientela e sui fattori che gli enti creditizi e gli istituti finanziari dovrebbero prendere in considerazione nel valutare i Rischi di riciclaggio associati ai singoli rapporti continuativi e alle operazioni occasionali («Orientamenti relativi ai fattori di Rischio di riciclaggio»), che abrogano e sostituiscono gli orientamenti JC/2017/37, recepiti dalla Banca d'Italia con Nota n. 15 del 4 ottobre 2021;
- Orientamenti EBA (European Banking Authority) - GL/2022/05 – del 14 giugno 2022, sulle politiche e le procedure relative alla gestione della conformità e al ruolo e alle responsabilità del responsabile antiriciclaggio ai sensi dell'articolo 8 e del capo VI della direttiva (UE) 2015/849” («Orientamenti EBA su Politiche e Procedure AML»). Con provvedimento del 1° agosto 2023 – pubblicato nella Gazzetta Ufficiale della Repubblica Italiana in data 16 agosto 2023 – la Banca d'Italia ha modificato le Disposizioni al fine di dare piena attuazione nel nostro ordinamento agli Orientamenti EBA su Politiche e Procedure;
- Orientamenti EBA (European Banking Authority) - GL/2022/15 – del 22 novembre 2022, sull'utilizzo di soluzioni di onboarding a distanza del cliente per le finalità di cui all'articolo 13, paragrafo 1, della direttiva (UE) 2015/849”, recepiti dalla Banca d'Italia con Nota n. 32 del 13 giugno 2023;
- Orientamenti EBA (European Banking Authority) - GL/2023/03 – del 31 marzo 2023, recanti modifiche agli orientamenti EBA/2021/02 ai sensi dell'articolo 17 e dell'articolo 18, paragrafo 4, della direttiva (UE) 2015/849 sulle misure di adeguata verifica della clientela e sui fattori che gli enti creditizi e gli istituti finanziari dovrebbero prendere in considerazione nel valutare i rischi di riciclaggio e finanziamento del terrorismo associati ai singoli rapporti continuativi e alle operazioni occasionali («Orientamenti relativi ai fattori di rischio di ML/TF») («Orientamenti EBA sui clienti che sono organizzazioni senza scopo di lucro»);
- Orientamenti EBA (European Banking Authority) - GL/2023/04 – del 31 marzo 2023, sulle politiche e sui controlli per la gestione efficace dei rischi di riciclaggio e finanziamento del terrorismo (ML/TF) nel fornire accesso ai servizi finanziari”, («Orientamenti EBA sul derisking»);
- Orientamenti EBA (European Banking Authority) - GL/2024/11– del 4 luglio 2024, sugli obblighi di informazione relativi ai trasferimenti di fondi e determinate cripto-attività ai sensi del regolamento (UE) 2023/1113 («Orientamenti sulla cd. “travel rule”»);
- Orientamenti EBA (European Banking Authority) - GL/2024/14 – del 14 novembre 2024, in materia di politiche, procedure e controlli interni atti a garantire l'attuazione di misure restrittive dell'Unione e nazionali.

Normativa nazionale

- Decreto Legislativo 22 giugno 2007 n. 109 recante misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale (per brevità “D.Lgs. 109/07”);
- Decreto Legislativo 21 novembre 2007 n. 231 e successive modifiche e integrazioni recante attuazione della normativa europea in materia di prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo (per brevità “D.Lgs. 231/07”);

- Decreto del Ministero dell'Economia e delle Finanze 11 marzo 2022 n. 55 recante disposizioni in materia di comunicazione, accesso e consultazione dei dati e delle informazioni relativi alla titolarità effettiva di imprese dotate di personalità giuridica, persone giuridiche private, trust produttivi di effetti giuridici rilevanti ai fini fiscali e istituti giuridici affini al trust.
- Decreto Legislativo 31 dicembre 2025 n. 210 recante modifiche al D.Lgs. 231/07 in materia di registri dei titolari effettivi;
- Decreto Legislativo 30 dicembre 2025 n. 211, in attuazione della direttiva 2024/1226/UE del Parlamento europeo e del Consiglio, del 24 aprile 2024, relativa alla definizione dei reati e delle sanzioni per la violazione delle misure restrittive dell'Unione e che modifica la direttiva (UE) 2018/1673.

Disposizioni delle Autorità di vigilanza nazionali

- Disposizioni di Vigilanza per le banche emanate da Banca d'Italia con Circolare n. 285 del 17 dicembre 2013 e successive modifiche e integrazioni, con particolare riferimento al sistema dei controlli interni, al sistema informativo e alla continuità operativa;
- Disposizioni in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e finanziamento del terrorismo emanate da Banca d'Italia il 26 marzo 2019 e successive modifiche e integrazioni (di seguito "Disposizioni sull'organizzazione");
- Istruzioni in materia di comunicazioni oggettive emanate dall'Unità di Informazione Finanziaria (UIF) il 28 marzo 2019 (di seguito "Istruzioni su comunicazioni oggettive");
- Disposizioni in materia di adeguata verifica della clientela emanate da Banca d'Italia il 30 luglio 2019 e successive modifiche e integrazioni (di seguito "Disposizioni AV");
- Disposizioni specifiche per la conservazione e l'utilizzo dei dati e delle informazioni a fini antiriciclaggio e di contrasto al finanziamento del terrorismo emanate da Banca d'Italia il 20 marzo 2020 (di seguito "Disposizioni sulla conservazione");
- Provvedimento di Banca d'Italia del 27 maggio 2009 recante indicazioni operative per l'esercizio di controlli rafforzati contro il finanziamento dei programmi di proliferazione di armi di distruzione di massa;
- Provvedimento UIF del 25 agosto 2020 recante disposizioni attuative per l'invio delle Segnalazioni Antiriciclaggio Aggregate – SARA (di seguito "Provvedimento SARA");
- Comunicazione UIF del 24 marzo 2022 sui depositi russi e bielorusi ai sensi dei Regolamenti (UE) 328/2022 e 398/2022;
- Provvedimento UIF del 12 maggio 2023 recante indicatori di anomalia per l'individuazione delle operazioni sospette;
- Provvedimento UIF del 18 dicembre 2025 recante nuove istruzioni sulle segnalazioni di operazioni sospette;
- Schemi rappresentativi di comportamenti anomali emanati dalla UIF;
- Casistiche di riciclaggio e finanziamento del terrorismo riportate nei Quaderni e nelle Analisi e Studi della UIF;
- Aggiornamenti dei codici ATECO 2025 per gli adempimenti AML.

1.2.2 NORMATIVA INTERNA

La presente *Policy AML* si inserisce nel set degli atti di normativa interna adottati dagli organi aziendali per il contrasto del riciclaggio e del finanziamento del terrorismo. Per la descrizione dettagliata delle soluzioni organizzative adottate e dell'impianto di prevenzione e contrasto del riciclaggio si fa rinvio ai seguenti documenti:

- Regolamento Antiriciclaggio;
- Manuale antiriciclaggio;
- Regolamento della Funzione Antiriciclaggio e del Responsabile SOS;
- Regolamento per la segnalazione delle operazioni sospette;
- Regolamento dei flussi informativi;
- Sistema dei controlli interni.

1.3 DEFINIZIONI

Si riportano di seguito definizioni rilevanti per la corretta interpretazione e applicazione della presente *Policy AML*.

Alto Dirigente: un amministratore o il direttore generale o altro dipendente delegato dall'organo con funzione di gestione o dal direttore generale a seguire i rapporti con la clientela a rischio elevato; l'alto dirigente ha una conoscenza idonea del livello di rischio di riciclaggio o di finanziamento del terrorismo cui è esposto il destinatario ed è dotato di un livello di autonomia sufficiente ad assumere decisioni in grado di incidere su questo livello di rischio.

AML (Anti Money Laundering / Combating Terrorism Finangiung): contrasto al riciclaggio e al finanziamento del terrorismo.

Approccio basato sul rischio: indica un approccio in base al quale le autorità competenti e le imprese individuano, valutano e comprendono i rischi di ML/TF a cui le imprese sono esposte e adottano misure di AML/CFT commisurate a tali rischi.

Archivi standardizzati: archivi mediante i quali sono resi disponibili i dati e le informazioni previsti dalle "Disposizioni per la conservazione e la messa a disposizione dei documenti, dei dati e delle informazioni per il contrasto del riciclaggio e del finanziamento del terrorismo" della Banca d'Italia; essi includono gli archivi unici informatici già istituiti alla data di entrata in vigore del decreto legislativo 25 maggio 2017, n. 90;

Archivio Unico Informatico c.d. AUI: un archivio, formato e gestito a mezzo di sistemi informatici, nel quale sono conservate in modo accentrato tutte le informazioni acquisite nell'adempimento degli obblighi di adeguata verifica, secondo i principi previsti nel Decreto Antiriciclaggio e nei provvedimenti attuativi emanati dalla Banca d'Italia. Tra gli Archivi standardizzati, l'AUI è l'archivio utilizzato dalla Banca.

Banca di comodo: la banca o l'ente che svolge funzioni analoghe a una banca che non ha una struttura organica e gestionale significativa nel paese in cui è stato costituito e autorizzato all'esercizio dell'attività, né è parte di un gruppo finanziario soggetto a un'efficace vigilanza su base consolidata.

Attività istituzionale: l'attività per la quale i destinatari hanno ottenuto l'iscrizione ovvero l'autorizzazione da parte di un'Autorità Pubblica.

Catena partecipativa complessa: struttura di proprietà e controllo con più di due livelli tra il Cliente e il Titolare effettivo, in cui risultano soddisfatte almeno due delle seguenti condizioni:

- esiste un accordo giuridico o un'entità giuridica simile, come una fondazione, in uno qualsiasi dei livelli sopra specificati;
- il Cliente e le entità giuridiche presenti in uno qualsiasi di questi livelli hanno sede in giurisdizioni al di fuori dell'UE;
- nella struttura sono coinvolti azionisti o amministratori fiduciari;
- la struttura oscura o riduce la trasparenza della proprietà senza alcuna motivazione o giustificazione economica legittima.

Cliente/Clientela: il soggetto che instaura o ha in essere rapporti continuativi o compie operazioni occasionali con i soggetti vigilati; in caso di rapporti continuativi o di operazioni occasionali cointestati a più soggetti, si considera cliente ciascuno dei cointestatari.

Congelamento di fondi: il divieto, in virtù dei regolamenti comunitari e della normativa nazionale, di movimentazione, trasferimento, modifica, utilizzo o gestione dei fondi o di accesso ad essi, così da modificarne il volume, l'importo, la collocazione, la proprietà, il possesso, la natura, la destinazione o qualsiasi altro cambiamento che consente l'uso dei fondi, compresa la gestione di portafoglio;

Congelamento di risorse economiche: il divieto, in virtù dei regolamenti comunitari e della normativa nazionale, di trasferimento, disposizione o, al fine di ottenere in qualsiasi modo fondi, beni o servizi, utilizzo delle risorse economiche, compresi, a titolo meramente esemplificativo, la vendita, la locazione, l'affitto o la costituzione di diritti reali di garanzia.

Controlli di linea (c.d. "controlli di primo livello"): controlli effettuati dalle strutture operative (ad es., controlli di tipo gerarchico, sistematici e a campione), anche attraverso unità dedicate esclusivamente a compiti di controllo che riportano ai responsabili delle strutture operative, ovvero eseguiti nell'ambito del back office, incorporati nelle procedure informatiche e diretti ad assicurare il corretto svolgimento delle operazioni.

Conti di passaggio: rapporti bancari di corrispondenza transfrontalieri, intrattenuti tra intermediari bancari e finanziari, utilizzati per effettuare operazioni in nome proprio e per conto della clientela.

Controparte/i: persone fisiche e giuridiche che instaurano una relazione d'affari (diversa dai rapporti contrattuali di durata rientranti nell'esercizio dell'attività istituzionale degli intermediari finanziari e degli altri soggetti esercenti attività finanziaria) con la Banca (anche se non destinatarie degli obblighi di cui al Decreto Antiriciclaggio).

Criptoattività: valori digitali registrati su un registro elettronico (*distributed ledger*) trasferibili, conservabili e utilizzabili per finalità di pagamento, investimento o come rappresentazione di diritti, inclusi token digitali e criptovalute, come definiti dal Regolamento (UE) 2023/1113 e dalla Direttiva (UE) 2018/843 (V Direttiva AML).

Criptovaluta: una forma di criptoattività utilizzabile principalmente come mezzo di pagamento digitale decentralizzato, priva di emissione da parte di un'autorità centrale, trasferibile tramite reti crittografiche sicure.

Dati identificativi (del Cliente, del relativo Titolare effettivo e dell'Esecutore): il nome e il cognome, il luogo e la data di nascita, la residenza anagrafica e, ove diverso, il domicilio, e, ove assegnato, il codice fiscale del Cliente, e ove ne sia prevista l'assegnazione, anche il relativo Titolare effettivo e dell'Esecutore. Nel caso di soggetti diversi da persona fisica, la denominazione, la sede legale, il numero di iscrizione nel registro delle imprese ovvero nel registro delle persone giuridiche ove previsto.

Denaro contante o Contanti: le banconote e le monete metalliche, in euro o in valute estere, aventi corso legale.

Delegato alla segnalazione delle operazioni sospette: il soggetto designato dall'Organo con funzione di supervisione strategica della Banca, alla valutazione delle operazioni sospette e alla loro successiva trasmissione alla Unità di Informazione Finanziaria, qualora ritenute fondate.

Embargo: divieto di commercio e di scambio con Paesi destinatari di provvedimenti sanzionatori, finalizzato a isolare e mettere il loro governo in una difficile situazione politica ed economica interna.

Esecutore: il soggetto delegato ad operare in nome e per conto del Cliente o a cui siano comunque conferiti poteri di rappresentanza che gli consentano di operare in nome e per conto del Cliente.

Esponente Responsabile per l'antiriciclaggio: il componente dell'organo di amministrazione responsabile per l'antiriciclaggio, il quale costituisce il principale punto di contatto tra il Responsabile della Funzione Antiriciclaggio e gli Organi con funzione di supervisione strategica e di gestione, come individuato dalle Disposizioni della Banca d'Italia in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari a fini di riciclaggio e finanziamento del terrorismo in attuazione degli Orientamenti

EBA sulle politiche e procedure interne per la gestione della compliance antiriciclaggio e sul ruolo del responsabile antiriciclaggio.

Fattori di rischio: indicano le variabili, singolarmente o in combinazione, suscettibili di accrescere o ridurre il rischio di ML/TF derivante da singoli rapporti continuativi o operazioni occasionali.

Finanziamento del terrorismo: in conformità con l'art. 1, comma 1, lettera d), del decreto legislativo 22 giugno 2007, n. 109: "qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione di fondi e risorse economiche, in qualunque modo realizzata, destinati ad essere, direttamente o indirettamente, in tutto o in parte, utilizzati per il compimento di una o più condotte con finalità di terrorismo, secondo quanto previsto dalle leggi penali, ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette".

Fondi: le attività e utilità finanziarie di qualsiasi natura, inclusi i proventi da questi derivati, possedute, detenute o controllate, anche parzialmente, direttamente o indirettamente, o per interposta persona fisica o giuridica da parte di soggetti designati, o da parte di persone fisiche o giuridiche che agiscano per conto o sotto la direzione di questi ultimi (quali i contanti, gli assegni, i crediti pecuniari, le cambiali, gli ordini di pagamento e altri strumenti di pagamento, i depositi presso enti finanziari o altri soggetti, i saldi sui conti, i crediti e le obbligazioni di qualsiasi natura, i titoli negoziabili a livello pubblico e privato, gli strumenti finanziari come definiti nel Decreto legislativo 24 febbraio 1998, n. 58, gli interessi, i dividendi o altri redditi ed incrementi di valore generati dalle attività, il credito, il diritto di compensazione, le garanzie di qualsiasi tipo, le cauzioni e gli altri impegni finanziari, le lettere di credito, le polizze di carico e gli altri titoli rappresentativi di merci, i documenti da cui risulti una partecipazione in fondi o risorse finanziarie, tutti gli altri strumenti di finanziamento delle esportazioni, le polizze assicurative concernenti i rami vita, ecc.).

Funzione Antiriciclaggio: la funzione, parte integrante del Sistema dei controlli interni di secondo livello, deputata a prevenire e contrastare i fenomeni nonché la realizzazione di operazioni di riciclaggio e di finanziamento del terrorismo.

Funzioni Aziendali di Controllo: la Funzione Compliance, la Funzione Risk Management, la Funzione Antiriciclaggio, la Funzione Internal Audit.

Gruppo: il gruppo bancario di cui all'articolo 60 TUB e disposizioni applicative. Il Gruppo bancario Cambiano è costituito dalla Capogruppo, la Banca Cambiano 1884 SpA la quale controlla al 100% la Cambiano Leasing SpA ed una società immobiliare che non è soggetta ad obblighi AML.

Indicatori di anomalia: fattispecie rappresentative di operatività ovvero di comportamenti anomali posti in essere dalla clientela, finalizzate ad agevolare la valutazione, da parte dei soggetti obbligati, degli eventuali profili di sospetto di riciclaggio o di finanziamento del terrorismo.

Mezzi di pagamento: il denaro contante, gli assegni bancari e postali, gli assegni circolari e gli altri assegni a essi assimilabili o equiparabili quali gli assegni di traenza, i vaglia postali, gli ordini di accreditamento o di pagamento, le carte di credito e le altre carte di pagamento, le polizze assicurative trasferibili, le polizze di pegno e ogni altro strumento che permetta di trasferire, movimentare o acquisire, anche per via telematica, fondi, valori o disponibilità finanziarie.

Misure restrittive: misure restrittive adottate dall'Unione europea sulla base dell'articolo 29 del Trattato sull'Unione europea e dell'articolo 215 del Trattato sul funzionamento dell'Unione europea, quali le misure in materia di congelamento di fondi e di risorse economiche, i divieti riguardanti la messa a disposizione di fondi e risorse economiche, nonché le misure economiche e finanziarie settoriali e gli embarghi sulle armi e le misure adottate dagli Stati membri in conformità del relativo ordinamento giuridico nazionale (nella misura in cui si applicano agli enti finanziari).

Operatività: l'attività richiesta al destinatario o rilevata dallo stesso nell'ambito dell'apertura o dello svolgimento di un rapporto continuativo, dell'esecuzione di una o più operazioni.

Operazione: l'attività consistente nella movimentazione, nel trasferimento o nella trasmissione di mezzi di pagamento o nel compimento di atti negoziali a contenuto patrimoniale.

Operazione frazionata: un'operazione unitaria sotto il profilo del valore economico, di importo pari o superiore ai limiti stabiliti dal decreto antiriciclaggio, realizzata attraverso più operazioni, singolarmente inferiori ai predetti limiti, effettuate in momenti diversi e in un circoscritto periodo di tempo fissato in sette giorni, ferma restando la sussistenza dell'operazione frazionata quando ricorrano elementi per ritenerla tale.

Operazione occasionale: si intende l'operazione c.d. extra-conto o per cassa, ossia l'operazione non riconducibile a un rapporto continuativo in essere, che comporti la trasmissione o la movimentazione di mezzi di pagamento di importo pari o superiore a 15.000 euro. Come condiviso nell'ambito del sistema bancario, al fine di intercettare le operazioni occasionali frazionate, la soglia di rilevanza per l'applicazione degli obblighi di Adeguata Verifica sulle operazioni occasionali è fissata in euro 5.000.

Operazione sospetta: operazione che per caratteristiche, entità, natura e per collegamento con altre operazioni o per frazionamento della stessa o per qualsivoglia altra circostanza conosciuta in ragione delle funzioni esercitate, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, in base agli elementi acquisiti ai sensi del decreto antiriciclaggio, induce a ritenere, sospettare o ad avere motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa.

Operatività a distanza: l'operatività svolta senza la presenza fisica del cliente e del personale incaricato della Banca. Quando il cliente è un soggetto diverso da una persona fisica, si considera presente quando lo è l'esecutore.

Organi aziendali: il complesso degli Organi con funzioni di supervisione strategica (Consiglio di Amministrazione), di gestione (Direttore Generale o altro Organo cui è assegnata la funzione di gestione) e di controllo (Collegio Sindacale).

Organo con funzione di controllo: organo che verifica la regolarità dell'attività di amministrazione e l'adeguatezza degli assetti organizzativi e contabili della Società. In Banca Cambiano tale Organo coincide con il Collegio Sindacale.

Organo con funzione di gestione: organo aziendale o componenti di esso ai quali spettano o sono delegati compiti di gestione, ossia l'attuazione degli indirizzi deliberati nell'esercizio della funzione di supervisione strategica. Il direttore generale rappresenta il vertice della struttura interna e come tale partecipa alla funzione di gestione. In Banca Cambiano tale Organo coincide con il Direttore Generale.

Organo con funzione di supervisione strategica: organo nel quale si concentrano le funzioni di indirizzo e/o di supervisione della gestione sociale (ad esempio, mediante esame e delibera in ordine ai piani industriali o finanziari ovvero alle operazioni strategiche della Società). In Banca Cambiano tale Organo coincide con il Consiglio di Amministrazione.

Origine dei fondi: indica la provenienza dei fondi specificatamente impiegati in un rapporto continuativo o in una operazione occasionale.

Paesi a fiscalità privilegiata: Paesi non facenti parte del continente europeo non rientranti nelle definizioni di Paesi Terzi ad alto rischio, Paesi Terzi a rischio e non Equivalenti e Paesi aventi un regime fiscale privilegiato, per cui fiscalmente scatta l'inversione dell'onere della prova per la residenza, come individuati dal Decreto del MEF del 4 Maggio 19991 in vigore dal 24 febbraio 2014 e s.m.i..

¹ Si considerano fiscalmente privilegiati, ai fini dell'applicazione dell'art. 2, comma 2-bis del testo unico delle imposte sui redditi, i seguenti Stati e territori: Alderney (Aurigny); Andorra (Principat d'Andorra); Anguilla; Antigua e Barbuda (Antigua and Barbuda); Antille Olandesi (Nederlandse Antillen); Aruba; Bahama (Bahamas); Bahrein (Dawlat al-Bahrain); Barbados; Belize; Bermuda; Brunei (Negara Brunei Darussalam); (Paese eliminato dalla lista ai sensi dell'art. 2 decreto 27 luglio 2010); Costa Rica (Republica de Costa Rica); Dominica; Emirati Arabi Uniti (Al-Imarat al-'Arabiya al Muttahida); Ecuador (Repuplica del Ecuador); Filippine (Pilipinas); Gibilterra (Dominion of Gibraltar); Gibuti (Djibouti); Grenada; Guernsey (Bailiwick of Guernsey); Hong Kong (Xianggang); Isola di Man (Isle of Man); Isole Cayman (The Cayman Islands); Isole Cook; Isole Marshall (Republic of the Marshall Islands); Isole Vergini Britanniche (British Virgin Islands); Jersey; Libano (Al-Jumhuriya al Lubnaniya); Liberia (Republic of Liberia); Liechtenstein (Furstentum Liechtenstein); Macao (Macao); Malaysia (Persekutuan Tanah Malaysia); Maldive (Divehi); (Paese eliminato dalla lista ai sensi dell'art. 2 decreto 27 luglio 2010); Maurizio (Republic of Mauritius); Monserrat; Nauru (Republic of Nauru); Niue; Oman (Saltanat 'Oman); Panama (Republica de Panama); Polinesia Francese (Polynesie Francaise); Monaco (Principaute' de Monaco); Sark (Sercq); Seicelle (Republic of Seychelles); Singapore (Republic of Singapore); Saint Kitts e Nevis (Federation of Saint Kitts and Nevis); Saint Lucia; Saint Vincent e Grenadine (Saint Vincent

Paesi comunitari: paesi appartenenti allo Spazio economico europeo.

Paesi o territori a rischio: comprendono i Paesi Terzi ad alto rischio, Paesi Terzi a rischio e non Equivalenti e Paesi a fiscalità privilegiata.

Paesi terzi: paesi non appartenenti allo Spazio economico europeo.

Paesi terzi ad alto rischio: Paesi non appartenenti all'Unione europea i cui ordinamenti presentano carenze strategiche nei rispettivi regimi nazionali di prevenzione del riciclaggio e del finanziamento del terrorismo, come individuati dalla Commissione europea nell'esercizio dei poteri di cui agli articoli 9 e 64 della Direttiva (UE) 2015/849. La Banca ha individuato tali paesi nella lista redatta dalla Commissione Europea² (come di volta in volta aggiornata), considerando, prudenzialmente anche tutti i paesi presenti nella lista anche se tale classificazione non è ancora in vigore. Inoltre, prudenzialmente sono inseriti tutti i paesi presenti nella lista *Jurisdictions with strategic deficiencies* del GAFI³.

Paesi Terzi Equivalenti: paesi non appartenenti allo Spazio economico europeo i cui ordinamenti non presentano carenze strategiche nei rispettivi regimi nazionali di prevenzione del riciclaggio e del finanziamento del terrorismo.

Pagamenti digitali: tutte le transazioni effettuate mediante strumenti di pagamento elettronici, inclusi bonifici online, carte di pagamento, portafogli elettronici (wallet) e altri strumenti di pagamento innovativi, come definiti dalla Direttiva (UE) 2015/2366 (PSD2) e successive modifiche.

Persone Esposte Politicamente (PEP):

1) una persona fisica che ricopre o ha ricoperto importanti cariche pubbliche comprendenti:

- 1.1 capi di Stato, capi di governo, ministri e viceministri o sottosegretari;
- 1.2 parlamentari o membri di organi legislativi analoghi;
- 1.3 membri degli organi direttivi di partiti politici;
- 1.4 membri delle corti supreme, delle corti costituzionali e di altri organi giudiziari di alto livello le cui decisioni non sono soggette a ulteriore appello, salvo in circostanze eccezionali;
- 1.5 membri delle corti dei conti e dei consigli di amministrazione delle banche centrali;
- 1.6 ambasciatori, incaricati d'affari e ufficiali di alto grado delle forze armate;
- 1.7 membri degli organi di amministrazione, direzione o sorveglianza delle imprese di proprietà statale;
- 1.8 direttori, vicedirettori e membri dell'organo di gestione, o funzione equivalente, di organizzazioni internazionali.

2) sono familiari di persone politicamente esposte: i genitori, il coniuge o la persona legata in unione civile o convivenza di fatto o istituti assimilabili alla persona politicamente esposta, i figli e i loro coniugi nonché le persone legate ai figli in unione civile o convivenza di fatto o istituti assimilabili;

3) sono soggetti con i quali le persone politicamente esposte intrattengono notoriamente stretti legami:

3.1 le persone fisiche che abbiano notoriamente la titolarità effettiva congiunta di soggetti giuridici o di istituti giuridici o qualsiasi altro stretto rapporto d'affari con una persona politicamente esposta;

and the Grenadines); Svizzera (Confederazione Svizzera); Taiwan (Chunghua MinKuo); Tonga (Pule'anga Tonga); Turks e Caicos (The Turks and Caicos Islands); Tuvalu (The Tuvalu Islands); Uruguay (Republica Oriental del Uruguay); Vanuatu (Republic of Vanuatu); Samoa (Independent State of Samoa).

²<https://www.consilium.europa.eu/en/policies/eu-list-of-non-cooperative-jurisdictions/>

https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-counteracting-financing-terrorism-international-level_en

³<https://www.fatf-gafi.org/en/topics/high-risk-and-other-monitored-jurisdictions.html>

<https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/increased-monitoring-february-2026.html>

<https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-february-2026.html>

3.2 le persone fisiche che siano uniche titolari effettive di soggetti giuridici o di istituti giuridici notoriamente creati di fatto a beneficio di una persona politicamente esposta.

Politici Italiani Locali (o PIL): soggetti che, pur non essendo PEP, operano in contesti strettamente attinenti alla vita politica locale e che, pertanto, presentano un potenziale rischio di riciclaggio superiore, individuati dalla Banca nelle seguenti figure: presidente di provincia, assessore provinciale e assessore comunale, sindaco di comune con popolazione inferiore a 15.000 abitanti.

Pubblica amministrazione: le amministrazioni pubbliche previste dall'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, gli enti pubblici nazionali, le società partecipate dalle amministrazioni pubbliche e dalle loro controllate, ai sensi dell'articolo 2359 del Codice civile, limitatamente alla loro attività di pubblico interesse disciplinata dal diritto nazionale o dall'Unione europea nonché i soggetti preposti alla riscossione dei tributi nell'ambito della fiscalità nazionale o locale, quale che ne sia la forma giuridica.

Rapporto continuativo: un rapporto contrattuale di durata, rientrante nell'esercizio dell'attività istituzionale del soggetto obbligato, che può dar luogo a più operazioni di trasferimento o movimentazione di mezzi di pagamento e che non si esaurisce in una sola operazione.

Riciclaggio, ai sensi dell'articolo 2, comma 4, del decreto antiriciclaggio:

- a) la conversione o il trasferimento di beni, effettuati essendo a conoscenza che essi provengono da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche delle proprie azioni;
- b) l'occultamento o la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o dei diritti sugli stessi, effettuati essendo a conoscenza che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività;
- c) l'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività;
- d) la partecipazione a uno degli atti previsti dalle lettere precedenti, l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolare l'esecuzione.

Rischio di riciclaggio:

- il rischio derivante dalla violazione di previsioni di legge, regolamentari e di autoregolamentazione funzionali alla prevenzione dell'uso del sistema finanziario per finalità di riciclaggio, di finanziamento del terrorismo o di finanziamento dei programmi di sviluppo delle armi di distruzione di massa, nonché
- il rischio di coinvolgimento in episodi di riciclaggio e di finanziamento del terrorismo o di finanziamento dei programmi di sviluppo delle armi di distruzione di massa.

Rischio inerente: nella logica del c.d. rischio "potenziale", la probabilità per la Società di subire un danno diretto od indiretto di natura sanzionatoria, penale, finanziaria o reputazionale senza considerare l'organizzazione ed il funzionamento dei propri presidi organizzativi ed il più generale Sistema dei controlli interni.

Rischio residuo: giudizio di sintesi che tiene conto della valutazione dell'idoneità dei presidi organizzativi, procedurali e di controllo in essere, con conseguente individuazione delle iniziative correttive da intraprendere ai fini della sua mitigazione.

Sistema dei controlli interni: l'insieme delle regole, delle funzioni, delle strutture, delle risorse dei processi e delle procedure che mirano ad assicurare, nel rispetto della sana e prudente gestione, le seguenti finalità:

- verifica dell'attuazione delle strategie e delle politiche aziendali;

- contenimento del rischio entro i limiti indicati nel quadro di riferimento per la determinazione della propensione al rischio della banca (Risk Appetite Framework - “RAF”);
- salvaguardia del valore delle attività e protezione dalle perdite;
- efficacia ed efficienza dei processi aziendali;
- affidabilità e sicurezza delle informazioni aziendali e delle procedure informatiche;
- prevenzione del rischio che la Banca sia coinvolta, anche involontariamente, in attività illecite (con particolare riferimento a quelle connesse con il riciclaggio, l’usura ed il finanziamento al terrorismo);
- conformità delle operazioni con la legge e la normativa di vigilanza, nonché con le politiche, i regolamenti e le procedure interne.

Strutture (o Unità) operative: le dipendenze territoriali della Banca; esse rappresentano il primo ed essenziale livello di presidio aziendale ai fini di prevenzione e contrasto dei fenomeni di riciclaggio e di finanziamento del terrorismo, cui competono concretamente l’amministrazione e la gestione dei rapporti con la clientela

Transaction monitoring: processo per l’analisi e la selezione delle operatività anomale basata su parametri quantitativi, quali l’importo o la frequenza delle operazioni e la provenienza o destinazione dei flussi, e qualitativi, quali la tipologia o le modalità di utilizzazione dei servizi e le caratteristiche dei soggetti coinvolti.

Titolare effettivo: la persona fisica o le persone fisiche, diverse dal Cliente, nell’interesse della quale o delle quali, in ultima istanza, il rapporto continuativo è istaurato, la prestazione professionale è resa o l’operazione è eseguita, ovvero, nel caso di soggetti diversi da persona fisica, la persona fisica o le persone fisiche cui, in ultima istanza, è attribuibile la proprietà diretta o indiretta dell’ente ovvero il relativo controllo.

UIF: l’Unità di Informazione Finanziaria per l’Italia.

2 ASSETTI DI GOVERNO, ORGANIZZAZIONE E CONTROLLI

2.1 SISTEMA ANTIRICICLAGGIO

Il sistema di prevenzione e contrasto al riciclaggio e finanziamento del terrorismo implementato dalla Banca si articola in strategie e politiche di gestione del rischio, assetti organizzativi, processi operativi, procedure interne, processi di identificazione, misurazione e controllo del rischio ML.

Ai sensi dell’art. 15 del D.Lgs. 231/07, l’impresa adotta procedure oggettive per l’analisi e la valutazione dei rischi di riciclaggio e di finanziamento del terrorismo. A tal fine, l’impresa tiene conto dei fattori di rischio associati alla tipologia di clientela, all’area geografica di operatività, ai canali distributivi e ai prodotti e i servizi offerti. L’impresa adotta i presidi e attua controlli e procedure adeguati alla propria natura e dimensione, necessari a mitigare e gestire i rischi di riciclaggio e di finanziamento del terrorismo.

Il Consiglio di Amministrazione definisce e riesamina annualmente gli orientamenti strategici in materia di gestione del rischio di riciclaggio, che devono risultare adeguati all’entità e alla tipologia del rischio cui è esposta l’impresa, misurato con il processo di *autovalutazione*.

In aderenza all’approccio basato sul rischio, le politiche devono risultare adeguate all’entità e alla tipologia dei profili di rischio cui è concretamente esposta l’attività della Banca.

L’*autovalutazione* costituisce il presupposto per la definizione e la manutenzione del Sistema Antiriciclaggio o Framework Antiriciclaggio, nell’ambito del più generale quadro di riferimento per la gestione dei rischi a cui si espone la Banca, espresso nel *RAF – Risk Appetite Framework*.

L’esercizio di *autovalutazione* è aggiornato con cadenza annuale e in caso di apertura di nuove linee di business.

Laddove emergano nuovi rischi di rilevante entità ovvero si verificano mutamenti significativi nei rischi esistenti, nell'operatività o nella struttura organizzativa o societaria, la Funzione AML attiva tempestivamente il processo di aggiornamento dell'esercizio di Autovalutazione, comunicando gli esiti al Consiglio di Amministrazione.

Gli esiti dell'esercizio di Autovalutazione, condotto per linea di business, sono dunque determinati in larga parte dalle scelte strategiche compiute dalla Banca con riferimento al modello industriale e distributivo, alle aree di sviluppo degli affari e alle politiche geografiche e di prodotto.

Gli orientamenti strategici per la gestione del rischio di riciclaggio e finanziamento del terrorismo-riconducibile ai rischi di non conformità, reputazionale e operativo, è declinata nel RAF Risk Appetite Framework mediante definizione dei livelli di risk appetite, di risk tolerance e di risk capacity.

Il sistema di prevenzione e contrasto al riciclaggio e finanziamento del terrorismo implementato dalla Banca, si basa sulle seguenti componenti o linee di azione:

- processo di autovalutazione del rischio di riciclaggio e finanziamento del terrorismo a cui è esposta la Banca
- politiche di gestione del rischio, calibrate di tempo in tempo sulla base dell'esposizione al rischio
- azione della Funzione Antiriciclaggio
- collaborazione attiva e processo di segnalazione delle operazioni sospette
- know your customer e processo di adeguata verifica della clientela
- gestione dei flussi informativi intraorgani e interfunzionali
- procedure interne aziendali per lo svolgimento dei processi operativi
- controlli interni di primo, secondo e terzo livello.

2.2 ASSETTO DI GOVERNO

2.2.1 CONSIGLIO DI AMMINISTRAZIONE

Il Consiglio di Amministrazione della Capogruppo è responsabile della definizione del complessivo modello di governo e gestione del rischio di riciclaggio e di finanziamento del terrorismo di Gruppo. È compito del Consiglio di Amministrazione della Capogruppo, a seguito del preventivo esame da parte del Collegio Sindacale, approvare la presente Policy AML di Gruppo ed il modello organizzativo per il governo e la gestione di tale rischio. Il Consiglio di Amministrazione della controllata è responsabile del recepimento e dell'attuazione delle strategie e delle politiche di gestione del rischio di riciclaggio e finanziamento del terrorismo internazionale definite a livello di Gruppo.

Di seguito i principali compiti del Consiglio di Amministrazione delle singole entità:

- definisce e riesamina periodicamente, gli orientamenti strategici e le politiche di governo dei rischi connessi con il riciclaggio e il finanziamento al terrorismo a cui è concretamente esposta la Banca; tali orientamenti strategici sono formalizzati nel *RAF – Risk Appetite Framework* e la valutazione del rischio cui è concretamente esposta l'impresa è formalizzata nella *Relazione sull'Autovalutazione* annualmente presentata al Consiglio dalla Funzione Antiriciclaggio;
- approva la *Policy AML* che illustra le scelte che la Banca compie sui vari profili rilevanti in materia di assetti organizzativi, procedure e controlli interni, adeguata verifica e conservazione dei dati, in coerenza con il principio di proporzionalità e con l'effettiva esposizione al rischio di riciclaggio;
- approva l'istituzione della funzione antiriciclaggio individuandone compiti e responsabilità, nonché modalità di coordinamento e di collaborazione con le altre funzioni aziendali di controllo;

- approva le linee di indirizzo di un sistema di controlli interni organico e coordinato, funzionale alla pronta rilevazione e alla gestione del rischio di riciclaggio e contrasto al finanziamento del terrorismo e ne assicura l'efficacia nel tempo;
- approva i principi per la gestione dei rapporti con la clientela classificata ad "alto rischio";
- nomina e revoca il responsabile antiriciclaggio, sentito l'organo con funzioni di controllo. La verifica del possesso dei requisiti deve risultare analiticamente nel verbale di nomina;
- nomina e revoca il responsabile delle segnalazioni di operazioni sospette, sentito l'organo con funzioni di controllo;
- assicura che i compiti e le responsabilità in materia antiriciclaggio e contrasto al finanziamento del terrorismo siano allocati in modo chiaro e appropriato, garantendo che le funzioni operative e quelle di controllo siano distinte e fornite di risorse qualitativamente e quantitativamente adeguate;
- assicura che sia approntato un sistema di flussi informativi adeguato, completo e tempestivo verso gli organi aziendali e tra le funzioni di controllo nonché un sistema di condivisione della documentazione che consenta agli organi aziendali accesso diretto alle relazioni delle funzioni di controllo in materia antiriciclaggio, alle pertinenti comunicazioni intercorse con le Autorità e alle misure di vigilanza imposte o alle sanzioni irrogate;
- assicura la tutela della riservatezza nell'ambito della procedura di segnalazione di operazioni sospette; con cadenza almeno annuale, esamina le relazioni relative all'attività svolta dal responsabile antiriciclaggio e sui controlli eseguiti dalle funzioni competenti, nonché il documento sui risultati dell'autovalutazione dei rischi di riciclaggio;
- con cadenza almeno annuale, valuta l'attività della Funzione antiriciclaggio e l'adeguatezza delle risorse umane e tecniche ad essa assegnate, anche alla luce della periodica verifica svolta dalla funzione di revisione interna;
- assicura che le carenze e le anomalie riscontrate in esito ai controlli di vario livello siano portate tempestivamente a sua conoscenza e promuove l'adozione di idonee misure correttive, delle quali valuta l'efficacia;
- valuta i rischi conseguenti all'operatività con paesi terzi associati a più elevati rischi di riciclaggio, individuando i presidi per attenuarli, di cui monitora l'efficacia;
- nomina l'esponente responsabile per l'antiriciclaggio e assicura che questi soddisfi le condizioni di cui alla normativa vigente; assicura, inoltre, che l'esponente responsabile per l'antiriciclaggio, una volta nominato, sia tempestivamente informato delle decisioni che possono incidere sull'esposizione di riciclaggio e finanziamento del terrorismo della Banca;
- procede all'identificazione, ai sensi dell'art. 22 comma 2 del Decreto Antiriciclaggio, della titolarità effettiva della Banca.

In aggiunta a quanto sopra riportato, il Consiglio di Amministrazione della Capogruppo ha i seguenti compiti:

- definisce e riesamina periodicamente gli orientamenti strategici e le politiche di governo dei rischi connessi con il riciclaggio e il finanziamento al terrorismo a cui è concretamente esposto il Gruppo;
- nomina e revoca il Responsabile Antiriciclaggio di Gruppo (anche "Responsabile AML di Gruppo"), sentito il Collegio Sindacale; il verbale di nomina deve contenere la verifica analitica del possesso dei requisiti di indipendenza, competenza, professionali e reputazionali e della disponibilità del tempo necessario all'efficace adempimento dei suoi compiti;
- nomina l'Esponente responsabile per l'antiriciclaggio di Gruppo (di seguito per brevità anche "Esponente AML di Gruppo"), coincidente con l'Esponente AML della Capogruppo, e assicura che questi soddisfi le condizioni previste alla Sezione III-bis delle Disposizioni sull'organizzazione.
- con cadenza almeno annuale, valuta l'attività della Funzione AML a livello di Gruppo e l'adeguatezza delle risorse umane e tecniche ad essa assegnate;

- approva la presente Policy AML di Gruppo.

2.2.2 DIRETTORE GENERALE

Il Direttore Generale cura l'attuazione degli indirizzi strategici e delle politiche di governo del Rischio di riciclaggio e finanziamento del terrorismo ed è responsabile per l'adozione di tutte le misure necessarie ad assicurare l'efficacia dell'organizzazione e del sistema dei controlli antiriciclaggio a tal fine esamina le proposte di interventi organizzativi e procedurali presentate dal responsabile della Funzione AML e formalizza, motivandola, l'eventuale decisione di non accoglierle. Nella predisposizione delle procedure operative, tiene conto delle indicazioni e delle linee guida emanate dalle autorità competenti e dagli organismi internazionali.

Il Direttore Generale definisce e cura l'attuazione di un sistema di controlli interni funzionale alla pronta rilevazione e alla gestione del rischio di riciclaggio e finanziamento del terrorismo e ne assicura l'efficacia nel tempo, in coerenza con gli esiti dell'esercizio di autovalutazione dei rischi; assicura che le procedure operative e i sistemi informativi consentano il corretto adempimento degli obblighi di adeguata verifica della Clientela e di conservazione dei documenti e delle informazioni.

In materia di segnalazione di operazioni sospette, il Direttore Generale definisce e cura l'attuazione di una Procedura adeguata alle specificità dell'attività, alle dimensioni e alle complessità della Banca, secondo il principio di proporzionalità e l'approccio basato sul rischio. La Procedura deve garantire certezza di riferimento, omogeneità nei comportamenti, applicazione generalizzata all'intera struttura, il pieno utilizzo delle informazioni rilevanti e la ricostruibilità dell'iter valutativo. Adotta, inoltre, misure volte ad assicurare il rispetto dei requisiti di riservatezza della Procedura di segnalazione, nonché strumenti adeguati per la rilevazione delle operazioni anomale.

Il Direttore Generale definisce e cura altresì l'attuazione delle iniziative e delle procedure necessarie per assicurare il tempestivo assolvimento degli obblighi di comunicazione alle Autorità previsti dalla normativa antiriciclaggio.

Inoltre:

- cura l'attuazione della presente Policy ed è responsabile per l'adozione di tutti gli interventi necessari ad assicurare l'efficacia dell'organizzazione e del sistema dei controlli antiriciclaggio;
- cura la definizione di un sistema di controlli interni funzionale alla pronta rilevazione e alla gestione del rischio di riciclaggio e di finanziamento del terrorismo e ne assicura l'efficacia nel tempo, in coerenza con le evidenze tratte dall'esercizio di autovalutazione dei rischi AML/CTF;
- assicura che le procedure operative e i sistemi informativi consentano il corretto adempimento degli obblighi di adeguata verifica della clientela e di conservazione dei documenti e delle informazioni;
- in materia di segnalazione di operazioni sospette, definisce e cura l'attuazione di una procedura adeguata alle specificità dell'attività, alle dimensioni e alla complessità della Banca, che garantisca certezza di riferimento, omogeneità nei comportamenti, applicazione generalizzata all'intera struttura, pieno utilizzo di tutte le informazioni rilevanti e la ricostruibilità dell'iter valutativo; adotta altresì le misure volte ad assicurare il rispetto dei requisiti di riservatezza della procedura di segnalazione nonché strumenti, anche informatici, per la rilevazione delle operazioni anomale;
- definisce e cura l'attuazione delle iniziative e delle procedure necessarie per assicurare il tempestivo assolvimento degli obblighi di comunicazione alle Autorità previsti dalla normativa antiriciclaggio;
- definisce e cura l'attuazione di procedure informative volte ad assicurare la conoscenza dei fattori di rischio a tutte le funzioni aziendali coinvolte e agli organi incaricati con funzione di controllo;
- definisce e cura l'attuazione delle procedure di gestione dei rapporti con la Clientela classificata ad "alto rischio", in coerenza con i principi fissati dall'organo di supervisione strategica;
- stabilisce i programmi di addestramento e formazione del personale sugli obblighi previsti dalla disciplina antiriciclaggio; l'attività di formazione deve rivestire carattere di continuità e sistematicità e tenere conto dell'evoluzione della normativa e delle procedure;
- stabilisce gli strumenti idonei a consentire la verifica dell'attività svolta dal personale in modo da rilevare eventuali anomalie che emergano, segnatamente, nei comportamenti, nella qualità delle

comunicazioni indirizzate ai referenti e alle strutture aziendali nonché nei rapporti del personale con la Clientela;

- assicura, nei casi di esternalizzazione dei compiti operativi della Funzione AML, il rispetto della normativa applicabile e riceve periodiche informazioni sullo svolgimento delle attività esternalizzate;
- nei casi in cui è necessaria la sua autorizzazione ai fini dell'instaurazione/proseguimento del rapporto ovvero al compimento dell'operazione, richiede il parere preventivo della Funzione AML;
- assicura, nei casi di operatività a distanza (e.g. effettuata attraverso canali digitali), l'adozione di specifiche procedure informatiche per il rispetto della normativa antiriciclaggio, con particolare riferimento all'individuazione automatica di operazioni anomale.

2.2.3 ESPONENTE RESPONSABILE PER L'ANTIRICICLAGGIO DELLE SINGOLE ENTITA'

Ferma restando la responsabilità collettiva degli organi aziendali, il Consiglio di Amministrazione nomina tra i propri componenti un Esponente responsabile per l'antiriciclaggio (di seguito anche l'“Esponente”).

L'esponente responsabile per l'antiriciclaggio viene nominato dal Consiglio di Amministrazione tra i propri componenti previa verifica del possesso dei seguenti requisiti: a) adeguate conoscenze, competenze ed esperienze concernenti i rischi di riciclaggio, le politiche, i controlli e le procedure antiriciclaggio e di contrasto al finanziamento del terrorismo nonché il modello di business della Società; b) dispone di tempo e risorse adeguate ad assolvere efficacemente ai propri compiti, fatto salvo quanto previsto dal Decreto Ministeriale del 23 novembre 2020, n. 169.

Il possesso delle adeguate conoscenze, competenze ed esperienze concernenti i rischi di riciclaggio e di finanziamento del terrorismo viene valutato dal Consiglio di Amministrazione sulla base di almeno uno dei seguenti criteri:

- esperienza come membro dell'organo di supervisione strategica, dell'organo di controllo di Società operanti nel settore bancario, finanziario e assicurativo;
- esperienza come Amministratore Delegato o Direttore Generale in Società operanti nel settore bancario, finanziario e assicurativo;
- esperienza in qualità di responsabile nel processo di individuazione, valutazione, monitoraggio, controllo e mitigazione delle principali tipologie di rischio di Società operanti nel settore bancario, finanziario e assicurativo;
- esperienza in qualità di responsabile di sistemi di controllo interno e altri meccanismi operativi di Società operanti nel settore bancario, finanziario e assicurativo;
- comprovata esperienza accademica o professionale in ambito antiriciclaggio.

La valutazione della disponibilità di tempo e risorse adeguate ad assolvere efficacemente ai compiti dell'esponente responsabile per l'antiriciclaggio viene svolta in base ai seguenti criteri:

- numero e tipologia di incarichi assunti (i.e. di Presidente del Consiglio di Amministrazione, esecutivi, non esecutivi, ecc.) presso altri intermediari bancari o finanziari e/o esistenza altri rapporti lavorativi o professionali di rilievo dell'Esponente;
- fabbisogno di tempo determinato al momento della nomina, sulla base della partecipazione preventivata alle riunioni del Consiglio di Amministrazione e a eventuali comitati, anche sulla base dei dati storici sulla frequenza e la durata delle riunioni, e comprensiva del tempo necessario per l'analisi della documentazione sottoposta a detti organi e della interlocuzione con le funzioni aziendali operative o di controllo;
- eventuali altre deleghe o incarichi assunti presso la Società (i.e. Amministratore Delegato, Responsabile della Funzione Antiriciclaggio, ecc.).

Ferme restando le ipotesi di potenziale conflitto di interesse previste in capo agli esponenti dalla disciplina anche regolamentare vigente ed, in particolare, quelle previste dalla “Policy per la gestione delle operazioni con soggetti collegati”, tra le altre ipotesi da valutarsi caso per caso, è possibile che sussista un conflitto di interesse nelle seguenti situazioni:

- svolgimento di incarichi operativi relativi alle decisioni sulla commercializzazione degli OICR;
- offerta di nuovi prodotti o servizi;
- nell'ambito dell'attività di conservazione dei dati e inoltro delle segnalazioni antiriciclaggio nei confronti delle Autorità di Vigilanza.

La presenza di un conflitto di interesse non indica di per sé che l'Esponente Responsabile per l'AML non possa essere considerato idoneo. Ciò si verifica solo se il conflitto di interesse pone un rischio rilevante e non sia possibile attenuare, gestire o prevenire adeguatamente il conflitto di interesse.

Al verificarsi di un conflitto di interesse rilevante in caso di fatti sopravvenuti, l'Esponente Responsabile per l'AML comunica la circostanza al Consiglio di Amministrazione che, a margine di una valutazione dettagliata, autorizza il protrarsi della situazione rilevata laddove non rilevi un difetto di indipendenza di giudizio individuando misure idonee ad attenuare, gestire o prevenire adeguatamente il conflitto di interesse, ovvero valuta di attribuire l'incarico di Esponente Responsabile per l'AML a un ulteriore membro del Consiglio di Amministrazione, idoneo per requisiti, competenza e disponibilità di tempo.

La Banca può individuare di volta in volta le misure più idonee ad attenuare, gestire o prevenire adeguatamente il conflitto di interesse, tra cui possono figurare la rimodulazione delle deleghe/competenze dell'Esponente Responsabile per l'AML, il monitoraggio da parte del Consiglio di Amministrazione per il tramite di flussi forniti dal Responsabile della Funzione Antiriciclaggio e/o dalla Funzione Antiriciclaggio, ovvero attraverso l'obbligo dell'Esponente Responsabile per l'AML di riferire al Consiglio di Amministrazione su eventuali situazioni di conflitto di interesse.

L'esponente responsabile per l'antiriciclaggio costituisce il principale punto di contatto tra il responsabile della funzione antiriciclaggio e gli organi con funzione di supervisione strategica e di gestione e assicura che questi ultimi dispongano delle informazioni necessarie per comprendere pienamente la rilevanza dei rischi di riciclaggio e finanziamento del terrorismo cui il destinatario è esposto, ai fini dell'esercizio delle rispettive attribuzioni.

L'esponente responsabile per l'antiriciclaggio:

- monitora che le politiche, le procedure e le misure di controllo interno in materia di antiriciclaggio e di contrasto al finanziamento del terrorismo siano adeguate e proporzionate, tenendo conto delle caratteristiche del destinatario e dei rischi cui esso è esposto;
- coadiuva il Consiglio di Amministrazione nelle valutazioni concernenti l'articolazione organizzativa e la dotazione di risorse della funzione antiriciclaggio, ivi compresa l'eventuale scelta di assegnare la responsabilità della funzione antiriciclaggio allo stesso esponente responsabile per l'antiriciclaggio;
- assicura che gli organi aziendali siano periodicamente informati in merito alle attività svolte dal responsabile della funzione antiriciclaggio nonché in merito alle interlocuzioni intercorse con le Autorità;
- informa gli organi aziendali delle violazioni e criticità concernenti l'antiriciclaggio di cui sia venuto a conoscenza e raccomanda le opportune azioni;
- verifica che il responsabile della funzione antiriciclaggio abbia accesso diretto a tutte le informazioni necessarie per l'adempimento dei propri compiti, disponga di risorse umane e tecniche e di strumenti sufficienti e sia informato su eventuali carenze relative all'antiriciclaggio individuate dalle altre funzioni di controllo interno e dalle autorità di vigilanza;
- assicura che le problematiche e le proposte di intervento rappresentate dal responsabile della funzione antiriciclaggio siano valutate dal Direttore Generale e dal Consiglio di Amministrazione.

2.2.4 ESPONENTE RESPONSABILE PER L'ANTIRICICLAGGIO DI GRUPPO

La capogruppo nomina un componente dell'organo di amministrazione quale esponente responsabile per l'antiriciclaggio a livello di gruppo. L'incarico ha natura esecutiva. L'esponente responsabile per l'antiriciclaggio costituisce il principale punto di contatto tra il responsabile della funzione antiriciclaggio di

gruppo e gli organi con funzione di supervisione strategica e di gestione della capogruppo e assicura che questi ultimi abbiano le informazioni necessarie per comprendere pienamente la rilevanza dei rischi di riciclaggio e di finanziamento del terrorismo cui il gruppo è esposto, ai fini dell'esercizio delle rispettive attribuzioni. L'esponente assicura che il responsabile della funzione antiriciclaggio di gruppo svolga in maniera efficace i propri compiti. I requisiti e dell'esponente per l'antiriciclaggio di gruppo sono i medesimi citati nel precedente paragrafo.

2.2.5 COLLEGIO SINDACALE

Il Collegio Sindacale all'interno di ciascuna entità, vigila sull'osservanza della normativa e sulla completezza, funzionalità e adeguatezza dei controlli antiriciclaggio e di contrasto al finanziamento del terrorismo.

Il Collegio Sindacale è sentito in merito alle decisioni concernenti la nomina del responsabile della funzione antiriciclaggio e del responsabile delle segnalazioni di operazioni sospette e nella definizione degli elementi dell'architettura complessiva del sistema di gestione e controllo del rischio di riciclaggio.

In particolare:

- si avvale delle strutture interne per lo svolgimento delle verifiche e dei necessari accertamenti;
- utilizza flussi informativi provenienti dagli altri Organi sociali, dal responsabile della funzione antiriciclaggio e da altre funzioni aziendali di controllo;
- valuta l'idoneità delle procedure per l'adeguata verifica della clientela, la conservazione delle informazioni e la segnalazione delle operazioni sospette;
- analizza i motivi delle carenze, anomalie e irregolarità riscontrate e promuove l'adozione delle opportune misure correttive.

Ai sensi dell'art. 46 del decreto antiriciclaggio, i componenti del Collegio Sindacale comunicano senza ritardo alla Banca d'Italia tutti i fatti di cui vengano a conoscenza nell'esercizio delle proprie funzioni che possano integrare violazioni gravi o ripetute o sistematiche o plurime delle disposizioni di legge applicabili e delle relative disposizioni attuative.

Nell'esercizio delle proprie attribuzioni, l'Organo con funzioni di controllo si avvale delle strutture interne per lo svolgimento delle verifiche e degli accertamenti necessari e utilizza flussi informativi provenienti dagli altri organi aziendali, dal responsabile antiriciclaggio e dalle altre funzioni di controllo interno.

2.2.6 ORGANISMO DI VIGILANZA EX D.LGS. 231/01

Il D.Lgs. 231/01 ascrive rilevanza al reato di riciclaggio e di finanziamento del terrorismo fra quelli da cui può discendere la responsabilità amministrativa della società.

Il fatto costituente reato di riciclaggio, o uno dei reati presupposto del riciclaggio e finanziamento del terrorismo richiamati dal D. Lgs. 231/01, commessi dalla persona fisica che agisce per conto della Banca, opera su un doppio piano:

- illecito penale ascrivibile all'individuo che lo ha commesso;
- illecito amministrativo ascrivibile alla società nell'interesse di cui è stato commesso o che ne ha tratto vantaggio.

La Banca, secondo i meccanismi di imputazione della responsabilità amministrativa dell'ente (differenziati in ragione della figura che commette il reato, apicale o sottoposto), potrebbe dunque essere responsabile a titolo autonomo per condotte riciclaggio di cui si accerti la rilevanza penale in sede giudiziaria.

Per garantire l'efficacia del modello organizzativo di cui al D.Lgs. 231/07, a fini esimenti di tale responsabilità amministrativa della società, risulta fondamentale l'attività dell'Organismo di Vigilanza che si avvale del supporto delle strutture aziendali. Per il monitoraggio del rischio di reato di riciclaggio e finanziamento del terrorismo o dei reati presupposto, sono previsti flussi informativi indirizzati all'OdV.

L'Organismo di vigilanza, infine, inoltra al responsabile SOS eventuali segnalazioni di operazioni sospette rilevate in modo autonomo nell'esercizio dei propri compiti.

2.2.7 FUNZIONE ANTIRICICLAGGIO

La Funzione antiriciclaggio (per brevità anche Funzione AML) è incaricata di sovrintendere all'attività di prevenzione e gestione dei rischi di riciclaggio. La Funzione AML rientra fra le funzioni di controllo di secondo livello e in quanto applicabili ad essa si applicano le norme della Circ. 285/13.

Essa supporta gli organi aziendali nella definizione di strategie per la gestione del rischio di riciclaggio, sulla base dei livelli di esposizione al rischio inerente e al rischio residuo, misurati all'esito il processo di autovalutazione.

Le scelte compiute dalle singole Entità sugli assetti organizzativi e sul posizionamento della Funzione AML rispondono al principio di proporzionalità, declinato nell'approccio basato sul rischio, in coerenza con il modello di business e le strategie adottate, con la natura, la dimensione, la complessità dell'attività svolta, con la tipologia e la gamma dei servizi prestati, con il numero e la tipologia di clienti, con la tipologia di canali di distribuzione, con l'elemento geografico; tengono conto, altresì, della strategia complessiva predisposta per la gestione del rischio di riciclaggio e di contrasto al finanziamento del terrorismo– oltre alle indicazioni contenute nel RAF, nel caso della Banca –, della struttura organizzativa aziendale (organigramma), degli assetti proprietari, nonché della forma giuridica e del numero di dipendenti, dell'appartenenza ad un Gruppo.

La Funzione AML riferisce sempre direttamente agli organi con funzione di supervisione strategica, di gestione e di controllo. Per la Banca ciò è assicurato dal collocamento gerarchico della Funzione Antiriciclaggio, che risponde direttamente al Consiglio di Amministrazione e al Collegio Sindacale.

La Funzione AML collabora con le altre funzioni di controllo e con le altre funzioni aziendali per sviluppare metodologie di gestione del rischio in modo coerente con le strategie e con l'operatività aziendale, al fine di garantire che i processi di lavoro siano conformi alla legislazione antiriciclaggio.

La Funzione AML verifica nel continuo che le procedure aziendali siano coerenti con l'obiettivo di prevenire e contrastare la violazione di norme antiriciclaggio. A tal fine, la funzione provvede a:

- identificare le norme applicabili e valutare il loro impatto sui processi e le procedure interne;
- collaborare alla definizione del sistema dei controlli interni e delle procedure finalizzati alla prevenzione e al contrasto dei rischi di riciclaggio;
- verificare nel continuo l'adeguatezza del processo di gestione dei rischi di riciclaggio e di finanziamento del terrorismo e l'idoneità del sistema dei controlli interni e delle procedure e proporre le modifiche organizzative e procedurali volte ad assicurare un adeguato presidio dei rischi di riciclaggio;
- condurre, in raccordo con il responsabile delle SOS, verifiche sulla funzionalità del processo di segnalazione e sulla congruità delle valutazioni effettuate dal primo livello sull'operatività della clientela;
- collaborare alla definizione delle politiche di governo del rischio di riciclaggio e finanziamento del terrorismo e delle varie fasi in cui si articola il processo di gestione di tale rischio;
- condurre, in raccordo con le altre funzioni aziendali interessate, l'esercizio annuale di autovalutazione dei rischi di riciclaggio e finanziamento del terrorismo a cui è esposto il destinatario e rendicontarne l'esito, annualmente, gli esiti agli organi aziendali;
- prestare supporto e assistenza agli organi aziendali e all'alta direzione;
- valutare in via preventiva il rischio di riciclaggio e finanziamento del terrorismo connesso all'offerta di prodotti e servizi nuovi, alla modifica significativa di prodotti o servizi già offerti, all'ingresso in un nuovo mercato o all'avvio di nuove attività e raccomandare le misure necessarie per mitigare e gestire questi rischi;

- verificare l'affidabilità del sistema informativo per l'adempimento degli obblighi di adeguata verifica della clientela, conservazione dei dati e segnalazione delle operazioni sospette;
- trasmettere mensilmente alla UIF i dati aggregati concernenti l'operatività complessiva del destinatario;
- trasmettere alla UIF, sulla base delle istruzioni dalla stessa emanate, le comunicazioni oggettive concernenti operazioni a rischio di riciclaggio;
- definire, d'accordo con il responsabile delle segnalazioni di operazioni sospette, procedure di gestione delle segnalazioni interne (provenienti dal cd. Primo livello) riguardanti situazioni di rischio particolarmente elevato da trattare con la dovuta urgenza;
- curare, in raccordo con le altre funzioni aziendali competenti in materia di formazione, la predisposizione di un adeguato piano di formazione, finalizzato a conseguire un aggiornamento su base continuativa del personale, e di indicatori di efficacia dell'attività di formazione svolta;
- informare tempestivamente gli organi aziendali di violazioni o carenze rilevanti riscontrate nell'esercizio dei relativi compiti;
- informare periodicamente gli organi aziendali – direttamente o per il tramite dell'esponente responsabile per l'antiriciclaggio, in base a quanto stabilito nella policy antiriciclaggio – circa lo stato di avanzamento delle azioni correttive adottate a fronte di carenze riscontrate nell'attività di controllo e circa l'eventuale inadeguatezza delle risorse umane e tecniche assegnate alla funzione antiriciclaggio e la necessità di potenziarle;
- definire, in collaborazione con le altre funzioni aziendali, metodologie di gestione del rischio in coerenti con le strategie e l'operatività aziendale e realizzare processi conformi alla normativa;
- svolgere le attività di adeguata verifica rafforzata della clientela nei casi in cui - per circostanze oggettive, ambientali o soggettive - è particolarmente elevato il rischio di riciclaggio;
- predisporre flussi informativi diretti agli organi aziendali, all'esponente responsabile per l'antiriciclaggio e all'alta direzione.
- effettuare le comunicazioni di infrazioni ex articolo 49 del decreto legislativo 231/2007 al Ministero dell'Economia e delle Finanze.

2.2.7.1 INQUADRAMENTO, CRITERI DI SELEZIONE E NOMINA DEL RESPONSABILE DELLA FUNZIONE AML

Il Responsabile AML è collocato in posizione gerarchico-funzionale adeguata, alle dirette dipendenze del Consiglio di Amministrazione e del Collegio Sindacale e riferisce agli Organi aziendali senza restrizioni o intermediazioni, ovvero per il tramite dell'Esponente AML.

In quanto rientrante nel novero dei responsabili di funzioni aziendali di controllo, il Responsabile AML non ricopre responsabilità dirette di aree operative né è gerarchicamente dipendente da soggetti responsabili di dette aree. Per aree operative si intendono, così come previsto dalla normativa antiriciclaggio, le aree nelle quali è prevista l'applicazione delle norme antiriciclaggio e contrasto al finanziamento del terrorismo e quindi si genera un rischio di non conformità alle stesse.

Per quanto concerne l'elemento reputazionale, il Responsabile AML deve possedere gli stessi requisiti di onorabilità prescritti per i componenti dell'Organo Amministrativo, e può comprovarli mediante autodichiarazione.

Al fine di verificare il possesso dei requisiti suddetti si applicano i seguenti criteri:

- a) indipendenza: intesa come l'autonomia organizzativa dalle strutture operative e di business direttamente coinvolte in attività in cui si manifestano i rischi di non conformità alla normativa antiriciclaggio o di coinvolgimento in episodi di riciclaggio;

- b) competenza e professionalità: la competenza e professionalità del Responsabile AML vengono valutate con riferimento all'esperienza da questi maturata in ambito AML (minimo 3 anni) ovvero alla formazione superiore specifica conseguita (es. master o formazione accademica);
- c) reputazione: reputazione è intesa come assenza di procedimenti penali e/o sanzionatori, condanne penali e/o amministrative da parte delle Autorità di Vigilanza a carico del soggetto interessato negli ultimi 10 anni, salvo il caso di delitti di natura colposa. La sussistenza di eventuali procedimenti e/o sanzioni di cui sopra sarà valutata dal Consiglio di Amministrazione sentito il Collegio Sindacale.

All'atto della nomina, nel rispetto dei requisiti fissati, il Consiglio di Amministrazione valuta l'idoneità a svolgere il ruolo di Responsabile della Funzione AML tenendo altresì in considerazione gli eventuali e ulteriori incarichi che questi ricopre e che deve preventivamente comunicare al Consiglio di Amministrazione.

Il personale chiamato eventualmente a collaborare con la Funzione Antiriciclaggio, anche se inserito in aree operative, riferisce direttamente al Responsabile della Funzione per le questioni attinenti a detti compiti.

2.2.7.2 CONTINUITÀ OPERATIVA DELLA FUNZIONE AML

In merito alla necessità di assicurare la continuità operativa della Funzione antiriciclaggio, individuando soluzioni organizzative per i casi di assenza del responsabile, così come richiesto dalle Disposizioni della Banca d'Italia, la Società individua e nomina la figura del sostituto del Responsabile Funzione AML in tutti i casi di assenza o impedimento di quest'ultimo.

Il soggetto nominato nel ruolo di sostituto del Responsabile Funzione AML è destinatario di tutte le attribuzioni previste per quest'ultimo dalle Disposizioni della Banca d'Italia e dalla presente Policy.

2.2.8 RESPONSABILE PER LE SEGNALAZIONI DI OPERAZIONI SOSPETTE

Il Consiglio di Amministrazione, sentito il Collegio Sindacale, ha conferito delega per la segnalazione di operazioni sospette al Responsabile Antiriciclaggio, che assume anche la carica di Responsabile SOS.

Il ruolo e le responsabilità del Responsabile SOS sono formalizzati e resi pubblici all'interno della Banca per quanto attiene al processo di segnalazione a UIF delle operazioni sospette e alle attività di valutazione del Responsabile SOS, mediante *Regolamento SOS*.

Il Responsabile SOS, tenuto conto del collocamento organizzativo, non ha responsabilità dirette in aree operative né risulta gerarchicamente dipendente da soggetti di dette aree.

Il responsabile delle segnalazioni di operazioni sospette:

- valuta, alla luce di tutti gli elementi disponibili, le operazioni sospette comunicate dal responsabile della dipendenza o di altro punto operativo o unità organizzativa o struttura competente alla gestione concreta dei rapporti con la clientela (cd. primo livello);
- valuta, alla luce di tutti gli elementi disponibili, le operazioni sospette di cui sia altrimenti venuto a conoscenza nell'ambito della propria attività;
- trasmette alla UIF le segnalazioni ritenute fondate, omettendo l'indicazione dei nominativi dei soggetti coinvolti nella procedura di segnalazione dell'operazione;
- mantiene evidenza delle valutazioni effettuate nell'ambito della procedura, anche in caso di mancato invio della segnalazione alla UIF.
- acquisisce ogni informazione utile dalla struttura che svolge il primo livello di analisi delle operazioni anomale e dalla funzione antiriciclaggio;
- ha libero accesso ai flussi informativi diretti agli Organi sociali e alle strutture e/o funzioni aziendali, significativi per la prevenzione e il contrasto del riciclaggio e del finanziamento del terrorismo (ad esempio, richieste pervenute dall'autorità giudiziaria o dagli organi investigativi);
- utilizza nelle valutazioni anche eventuali elementi desumibili da fonti informative liberamente accessibili;

- svolge un ruolo di interlocuzione con la UIF e corrisponde tempestivamente alle eventuali richieste di approfondimento provenienti dalla stessa.

2.2.9 FUNZIONE DI INTERNAL AUDIT

La funzione di revisione interna verifica in modo continuativo il grado di adeguatezza dell'assetto organizzativo aziendale e la sua conformità rispetto alla disciplina di riferimento e vigila sulla funzionalità del complessivo sistema dei controlli interni.

La funzione di revisione interna sottopone a verifica periodica l'adeguatezza e l'efficacia della funzione antiriciclaggio.

La Funzione Internal Audit, in materia di antiriciclaggio e di finanziamento al terrorismo, ha il compito di verificare:

- il costante rispetto dell'obbligo di adeguata verifica, sia nella fase di instaurazione del rapporto assicurativo che nello svilupparsi nel tempo della relazione;
- l'effettiva acquisizione e l'ordinata conservazione dei dati e documenti prescritti dalla normativa;
- l'effettivo grado di coinvolgimento del personale nonché dei responsabili delle strutture centrali e periferiche, nell'attuazione degli obblighi di comunicazione e segnalazione.

La funzione di revisione interna pianifica le verifiche in materia di rischi di riciclaggio, le quali interessano sia le strutture operative interne che la rete distributiva, nonché altri soggetti cui la Banca abbia esternalizzato specifiche attività che possono interessare anche il processo antiriciclaggio.

Le risultanze delle attività di intervento da parte dell'Internal Audit sono oggetto di condivisione con il Responsabile Antiriciclaggio.

La funzione di revisione interna svolge interventi di follow-up volti a verificare l'avvenuta adozione e l'efficacia degli interventi correttivi in ordine a carenze e irregolarità riscontrate nell'ambito delle verifiche e della loro idoneità a evitare analoghe situazioni in futuro.

Nell'ambito dell'esercizio di autovalutazione dei rischi di riciclaggio la funzione Internal Audit sottopone a revisione il processo almeno annualmente.

La funzione di revisione interna riporta, almeno annualmente, agli organi aziendali informazioni sull'attività svolta e sui suoi esiti, fermo restando il rispetto degli obblighi di riservatezza previsti dal decreto antiriciclaggio.

2.3 PRESIDIO DEL RISCHIO DI RICICLAGGIO NEL GRUPPO

2.3.1 INTEGRAZIONE NEL PRESIDIO DEL RISCHIO DI RICICLAGGIO

La Capogruppo del Gruppo Bancario Cambiano definisce gli indirizzi strategici in materia di gestione del rischio di riciclaggio.

Con specifico riguardo al rischio di riciclaggio, la Capogruppo assicura che gli organi aziendali delle altre società appartenenti al gruppo attuino nella propria realtà aziendale le strategie e le politiche di gruppo, al fine di sviluppare un approccio globale al rischio di riciclaggio.

La Banca, in ottemperanza alla normativa di vigilanza, definisce e approva politiche condivise per la gestione del rischio di riciclaggio e finanziamento del terrorismo e per l'adempimento degli obblighi previsti dalla normativa antiriciclaggio; a tal fine la Capogruppo assicura che gli organi delle società controllate adottino la presente *Policy AML*, con condivisione dei principi di gestione del rischio di riciclaggio e finanziamento del terrorismo e adesione alle linee guida qui riportate.

A tal fine, la Capogruppo, in ottemperanza alla normativa di vigilanza, ha definito e approvato:

- una metodologia di gruppo per la valutazione dei rischi di riciclaggio e finanziamento del terrorismo mediante processo di autovalutazione; a tal fine la Capogruppo assicura che gli organi delle società controllate assoggettate all'obbligo di autovalutazione adottino una metodologia di autovalutazione coerente con quella adottata dalla Capogruppo, in modo tale da consentire una sintesi dei risultati e cogliere gli elementi di rilievo per una stima complessiva dell'esposizione al rischio;
- politiche condivise per la gestione del rischio di riciclaggio e finanziamento del terrorismo e per l'adempimento degli obblighi previsti dalla normativa antiriciclaggio; a tal fine la Capogruppo assicura che gli organi delle società controllate adottino, con gli opportuni aggiustamenti anche in ossequio al principio di proporzionalità, la presente Policy AML, con condivisione dei principi di gestione del rischio ML e adesione alle linee guida qui riportate.

Tale coordinamento e condivisione in materia AML avviene, fra le altre, con le seguenti modalità:

- istituzione di una base informativa comune che consenta a tutte le società del Gruppo di valutare in modo omogeneo la clientela;
- adozione di un sistema di allerta per gestire il caso in cui un cliente condiviso sia stato profilato "alto" in maniera differente fra società del Gruppo, con adeguamento al profilo di rischio più elevato tra quelli assegnati;
- obbligo di comunicazione alle altre società nel caso in cui una società del gruppo intervenga con variazione del profilo di rischio ad "alto".

2.3.2 ESTERNALIZZAZIONE DELLA FUNZIONE ANTIRICICLAGGIO

Nel Gruppo viene applicato un *modello accentrato*, ciò significa che le società del Gruppo assoggettate alla disciplina antiriciclaggio hanno esternalizzato le attività della Funzione Antiriciclaggio alla Capogruppo.

Tale scelta garantisce lo stretto coordinamento nelle politiche di gestione del rischio di riciclaggio e finanziamento del terrorismo fra le società del Gruppo e piena uniformità e integrazione nelle modalità di presidio e di adempimento degli obblighi AML.

L'esternalizzazione delle attività riconducibili alla Funzione Antiriciclaggio è disciplinata nell'accordo di esternalizzazione stipulato fra Capogruppo e Controllate, in coerenza con quanto previsto nella *Politica aziendale in materia di esternalizzazione di funzioni aziendali* adottata dalla Banca in qualità di Capogruppo ai sensi della Circ. 285/13 emanata da Banca d'Italia.

2.4 PRESIDIO SULL'APPLICAZIONE DELLE MISURE RESTRITTIVE

In conformità alla Direttiva (UE) 2024/1226 e al relativo decreto di attuazione (D.Lgs. 211/2025), la Banca adotta un sistema di controllo volto a garantire l'osservanza delle misure restrittive (sanzioni finanziarie e commerciali) adottate dall'Unione Europea e dalle Nazioni Unite.

A tal fine, la Banca adotta i seguenti presidi:

- **Screening Dinamico e Monitoraggio delle Liste:** effettua un allineamento costante delle anagrafiche clienti, dei titolari effettivi e delle controparti dei pagamenti con le versioni più aggiornate delle *Sanction Lists*. Tale verifica viene effettuata:
 - in fase di instaurazione del rapporto;
 - su base continuativa;
 - preventivamente all'esecuzione di ogni operazione di bonifico o trasferimento fondi.
- **Gestione dei Falsi Positivi e Tracciabilità:** ogni occorrenza rilevata dai sistemi di screening viene analizzata per escludere casi di omonimia. Il processo di analisi, le motivazioni dello scarto di un "match" e la documentazione a supporto devono essere tracciati, conservati e messi a disposizione delle Autorità di Vigilanza, ove richiesto.
- **Congelamento Immediato dei Fondi e astensione:** al momento della pubblicazione di nuovi soggetti nelle liste restrittive (ONU/UE), la Banca procede senza indugio al congelamento di tutti i fondi e delle

risorse economiche detenuti, posseduti o controllati, anche per interposta persona, dai soggetti designati.

- **Obblighi Informativi e Trasparenza:** comunicazione all'Unità di Informazione Finanziaria (UIF) e al Comitato di sicurezza Finanziaria (CSF) ogni misura di congelamento applicata entro i termini previsti per legge.

L'esponente aziendale responsabile per l'attuazione delle misure restrittive, nominato dal Consiglio di Amministrazione, è incaricato di garantire l'efficacia dei controlli, il congelamento immediato dei fondi e il rispetto degli obblighi informativi verso le Autorità.

2.5 CONTROLLI INTERNI

2.5.1 PROFILI STRUTTURALI

Il Consiglio di Amministrazione, conformemente a quanto previsto dalle Disposizioni sull'Organizzazione, approva e riesamina periodicamente le linee di indirizzo del sistema dei controlli interni, assicurando che lo stesso sia organico, integrato e coerente con il modello di business della Banca, nonché idoneo a garantire la tempestiva individuazione, valutazione, gestione e mitigazione del rischio di riciclaggio e di finanziamento del terrorismo.

Il sistema dei controlli interni è definito in conformità al principio dell'approccio basato sul rischio (*risk-based approach*) ed è volto a garantire:

- la sana e prudente gestione della Banca;
- la conformità alle disposizioni normative e regolamentari applicabili;
- l'efficacia e l'efficienza dei processi aziendali;
- l'affidabilità e l'integrità delle informazioni.

Il Consiglio di Amministrazione assicura nel tempo l'adeguatezza e l'efficacia del sistema dei controlli interni, tenendo conto dell'evoluzione del contesto normativo, dei rischi emergenti e delle caratteristiche operative della Banca.

Il complessivo sistema dei controlli interni, sia a fini generali di conformità dei comportamenti alle regole, sia, nello specifico, a fini di contrasto dei rischi di riciclaggio e di finanziamento del terrorismo, è esteso a tutti i soggetti, ivi compresi gli esponenti aziendali, che possano entrare in contatto con i potenziali clienti.

Le concrete scelte adottate tengono conto dell'esigenza di dotarsi di una struttura snella, la quale, alla luce del principio di proporzionalità e secondo un principio di efficienza, favorisca la comunicazione fra le varie strutture e la tempestiva attivazione dei flussi informativi verso gli organi aziendali. Il dettaglio dei processi operativi è definito all'interno del Regolamento AML.

Tenuto conto delle valutazioni effettuate l'individuazione di rischio e in applicazione del principio di proporzionalità, la Banca struttura l'assetto dei presidi di prevenzione del riciclaggio e di contrasto al finanziamento del terrorismo come di seguito rappresentato.

Il modello dei controlli interni in ambito AML/CFT si fonda sui seguenti principi:

Controlli di primo livello (controlli di linea)

Le unità operative sono responsabili dei controlli di primo livello e del corretto svolgimento delle attività operative connesse alla relazione con la clientela.

In particolare, esse:

- assicurano la piena applicazione della normativa AML/CFT e delle procedure interne, con riferimento all'adeguata verifica della clientela, alla profilatura del rischio e al continuo aggiornamento delle informazioni;

- presidiano la corretta acquisizione, registrazione e conservazione dei dati e dei documenti, garantendone completezza, coerenza e tracciabilità;
- effettuano controlli preventivi e contestuali integrati nei processi, anche mediante l'utilizzo di sistemi informatici e controlli automatizzati;
- rilevano tempestivamente eventuali anomalie, incoerenze o scostamenti rispetto al profilo di rischio della clientela;
- attivano i flussi informativi verso la Funzione Antiriciclaggio per la valutazione delle operazioni potenzialmente sospette;
- collaborano attivamente al processo di segnalazione delle operazioni sospette.

Controlli di secondo livello

La Funzione Antiriciclaggio è una funzione indipendente di controllo di secondo livello, dotata di adeguata autonomia, risorse e competenze, responsabile del presidio complessivo del rischio di riciclaggio e finanziamento del terrorismo.

La Funzione AML svolge attività di indirizzo, supporto e verifica, finalizzate ad assicurare l'adeguatezza e l'efficacia dei presidi aziendali.

In particolare:

- coordina il processo di autovalutazione del rischio di riciclaggio, contribuendo alla determinazione del rischio inerente e residuo;
- monitora nel continuo l'esposizione al rischio di riciclaggio e finanziamento del terrorismo mediante indicatori e metriche coerenti con il Risk Appetite Framework (RAF);
- svolge controlli di conformità ex ante su processi, procedure e prodotti, assicurando il presidio del processo di recepimento delle novità normative;
- verifica nel continuo l'efficacia e l'adeguatezza dei presidi AML, anche tramite controlli tematici, analisi a campione e verifiche in loco;
- valuta l'affidabilità e la funzionalità dei sistemi informativi a supporto degli adempimenti AML;
- presidia il processo di transaction monitoring, verificando l'efficacia degli scenari di rischio, la gestione degli alert e la coerenza dei modelli utilizzati;
- supporta le strutture operative e gli organi aziendali mediante attività consulenziale e di formazione;
- promuove la diffusione della cultura del rischio e della compliance all'interno della Banca.

Controlli di terzo livello

La Funzione Internal Audit verifica, nel continuo, il grado di adeguatezza dell'assetto organizzativo aziendale e la sua conformità rispetto alla disciplina di riferimento e vigila sulla funzionalità del complessivo sistema dei controlli interni.

Attraverso controlli sistematici, anche di tipo ispettivo, la Funzione Internal Audit verifica inoltre:

- il costante rispetto dell'obbligo di adeguata verifica, sia nella fase di instaurazione del rapporto sia nello svilupparsi nel tempo della relazione;
- l'effettiva acquisizione e l'ordinata conservazione dei dati e dei documenti, secondo quanto previsto dalla normativa;
- l'allineamento tra la procedura contabile di gestione e quella di alimentazione e gestione dell'AUI della Banca;
- l'effettivo grado di coinvolgimento del personale nonché dei responsabili delle strutture centrali e periferiche, nell'attuazione degli obblighi di comunicazione e segnalazione.

Gli interventi, sia a distanza che ispettivi, inseriti nel piano annuale della Funzione Internal Audit, approvato dal Consiglio di Amministrazione, sono oggetto di pianificazione per consentire che tutte le strutture operative siano sottoposte a verifica in un congruo arco di tempo. Tali iniziative sono più frequenti nei confronti delle strutture maggiormente esposte ai rischi di riciclaggio, nonché con riferimento ai rapporti con profilo di rischio alto.

La Funzione Internal Audit svolge, altresì, interventi di follow-up al fine di assicurarsi dell'avvenuta adozione degli interventi correttivi delle carenze e irregolarità riscontrate e della loro idoneità a evitare analoghe situazioni nel futuro.

2.5.2 COORDINAMENTO FRA FUNZIONI DI CONTROLLO IN MATERIA AML

La collaborazione tra la Funzione Antiriciclaggio e le altre Funzioni di controllo si inserisce nel più generale quadro di coordinamento tra tutte le strutture con compiti di controllo al fine di assicurare il corretto funzionamento del sistema dei controlli interni, sulla base di una proficua interazione, evitando sovrapposizioni o carenze di presidio.

Il contributo alla creazione di valore da parte della Funzione Antiriciclaggio risulta tanto maggiore quanto più forti sono le sinergie realizzate con gli altri attori del sistema dei controlli interni.

L'interazione e il coordinamento della Funzione AML con le altre Funzioni di controllo è altresì assicurata:

- da una pianificazione condivisa e organica del piano di lavoro annuale delle funzioni di controllo;
- da una condivisione e congiunta lettura critica degli esiti delle verifiche svolte da ciascuna funzione di controllo in materia AML;
- dallo scambio di adeguati flussi informativi fra le funzioni di controllo;
- dalla partecipazione condivisa al Comitato rischi;
- dal confronto congiunto e periodico con l'Organismo di Vigilanza sulle materie AML;
- dall'opera di raccordo e supervisione svolta dal Collegio Sindacale.

2.5.3 SISTEMA DI WHISTLEBLOWING

In conformità a quanto previsto dall'art. 48 del D.Lgs. 231/2007 e dalle disposizioni di vigilanza emanate dalla Banca d'Italia, la Banca ha adottato un sistema interno di segnalazione delle violazioni (c.d. *whistleblowing*) volto a consentire al personale e agli altri soggetti individuati dalla normativa applicabile di segnalare, anche in forma anonima, comportamenti, atti od omissioni che possano costituire violazione delle disposizioni normative o interne, incluse quelle in materia di prevenzione del riciclaggio e del finanziamento del terrorismo.

Il sistema di segnalazione è disciplinato in conformità alle disposizioni contenute nella Circolare n. 285/2013 della Banca d'Italia e nella normativa whistleblowing vigente, e garantisce:

- la riservatezza dell'identità del segnalante, del soggetto segnalato e dei soggetti comunque menzionati nella segnalazione, fatti salvi gli obblighi di legge e le esigenze connesse allo svolgimento delle indagini o dei procedimenti avviati dalle Autorità competenti;
- la protezione del segnalante da qualsiasi forma di ritorsione, discriminazione o penalizzazione conseguente alla segnalazione effettuata in buona fede;
- la presenza di canali di segnalazione dedicati, specifici e indipendenti, idonei a garantire la sicurezza e la riservatezza delle informazioni trasmesse;
- la gestione delle segnalazioni da parte di strutture aziendali indipendenti, nel rispetto dei principi di imparzialità, tracciabilità e conservazione delle informazioni.

Le segnalazioni relative a possibili violazioni della normativa antiriciclaggio e di contrasto al finanziamento del terrorismo sono pertanto trattate nell'ambito del sistema interno di whistleblowing adottato dalla Banca, che si affianca, senza sostituirla, alle ulteriori procedure previste dall'ordinamento in specifici ambiti normativi, tra cui:

- le segnalazioni all'Organismo di Vigilanza ai sensi del Decreto Legislativo 231/2001 con riferimento ai reati presupposto;
- le segnalazioni di operazioni sospette effettuate ai sensi della normativa antiriciclaggio.

Le modalità operative di utilizzo dei canali di segnalazione e di gestione delle segnalazioni sono disciplinate da apposita normativa interna e portate a conoscenza di tutto il personale.

3 ADEGUATA VERIFICA

3.1 NOZIONI CHIAVE SULL'ADEGUATA VERIFICA

L'adeguata verifica o per brevità "AV" o *customer due diligence*, rappresenta un istituto centrale nella normativa antiriciclaggio e di contrasto al finanziamento del terrorismo posti a carico della Banca.

L'adeguata verifica consiste in un processo composto di molteplici attività, da realizzarsi all'avvio della relazione con il cliente e nel continuo, per tutta la durata del rapporto.

3.1.1 APPROCCIO BASATO SUL RISCHIO

Le misure di Adeguata Verifica sono proporzionate in relazione al livello di rischio di riciclaggio e finanziamento del terrorismo assegnato al cliente in fase di conoscenza iniziale e nel continuo.

In applicazione del principio di *risk based approach*, la Banca modula le attività di adeguata verifica calibrando gli adempimenti in base al rischio associato al cliente, al rapporto di affari, al prodotto o alla transazione di cui trattasi. Le misure di adeguata verifica sono così graduate su tre macro - livelli:

- adempimenti ordinari
- adempimenti rafforzati
- adempimenti semplificati.

Le misure di adeguata verifica della clientela mirano ad ottenere una conoscenza approfondita del cliente, del contesto socio economico in cui opera, dei suoi legami, dei rapporti che intrattiene con la banca e delle operazioni che realizza.

3.1.2 OBBLIGHI DI ADEGUATA VERIFICA

Ai sensi delle *Disposizioni su Adeguata Verifica* emanate da Banca d'Italia, il processo di adeguata verifica si compone delle seguenti attività, che incorporano specifici obblighi:

- a) identificazione del cliente e dell'eventuale esecutore;
- b) identificazione dell'eventuale titolare effettivo;
- c) verifica dell'identità del cliente, dell'eventuale esecutore e dell'eventuale titolare effettivo, sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente;
- d) acquisizione e valutazione di informazioni sullo scopo e sulla natura prevista del rapporto nonché, in presenza di un rischio elevato di riciclaggio e di finanziamento del terrorismo, dell'operazione occasionale;
- e) esercizio di un controllo costante nel corso del rapporto continuativo.

Quando la Banca non è in grado di rispettare gli obblighi di adeguata verifica della clientela non instaura il rapporto continuativo ovvero non esegue l'operazione. Se tale impossibilità si verifica per un rapporto continuativo in essere, essa si astiene dal proseguire il rapporto. In questi casi, occorre valutare, inoltre, se inviare una segnalazione di operazione sospetta.

Ai sensi delle *Disposizioni su Adeguata Verifica* emanate da Banca d'Italia, le attività di adeguata verifica sono effettuate almeno nei momenti e nelle circostanze di seguito indicati:

- quando si instaura un rapporto continuativo;

- quando viene eseguita un'operazione occasionale disposta dal cliente, che comporti la trasmissione o la movimentazione di mezzi di pagamento di importo pari o superiore a 15.000 euro, indipendentemente dal fatto che sia effettuata con un'operazione unica o con più operazioni frazionate;
- quando vi è sospetto di riciclaggio, indipendentemente da qualsiasi deroga, esenzione o soglia applicabile, avvalendosi anche degli indicatori di anomalia e degli schemi rappresentativi di comportamenti anomali emanati dall'UIF in base al decreto antiriciclaggio;
- quando sorgano dubbi sulla completezza, attendibilità o veridicità delle informazioni o della documentazione precedentemente acquisite dalla clientela (es., nel caso di mancato recapito della corrispondenza all'indirizzo comunicato o di incongruenze tra documenti presentati dal cliente o comunque acquisiti dal destinatario).

La raccolta delle notizie e dei dati avviene attraverso il processo informatico guidato della compilazione del Questionario KYC – know your customer. Resta fermo che, costituendo parte integrante del processo di analisi della clientela svolto dalla Banca ai fini dell'avvio o del mantenimento dei rapporti, l'adeguata verifica si considera tracciata mediante l'acquisizione delle informazioni rilevanti e dei documenti che compongono il fascicolo del cliente e del rapporto intrattenuto con la Banca. Tali fascicoli sono conservati presso le dipendenze o unità operative incaricate della gestione del rapporto.

3.1.3 OPERATIVITÀ A DISTANZA

Per operatività a distanza si intende quella svolta senza la compresenza fisica, presso il destinatario, del cliente, dei dipendenti del destinatario o di altro personale incaricato dal destinatario; quando il cliente è un soggetto diverso da una persona fisica, esso si considera presente quando lo è l'esecutore.

La normativa richiede di porre particolare attenzione a questa operatività, in quanto la Banca non ha un contatto diretto con il cliente ed è quindi necessario accertare l'identità del cliente tramite documenti, dati o informazioni supplementari.

La Banca adotta soluzioni di onboarding a distanza solo per alcuni dei prodotti offerti. In particolare, l'operatività a distanza è prevista nell'ambito dell'apertura di un conto corrente e/o carta di debito ed è riservato alle Persone Fisiche.

Nell'operatività a distanza, ed in particolare nell'ambito delle soluzioni di onboarding, la Banca tiene conto delle previsioni degli "Orientamenti dell'Autorità bancaria europea sull'utilizzo di soluzioni di onboarding a distanza del cliente per le finalità di cui all'articolo 13, paragrafo 1, della direttiva (UE) 2015/849 (EBA/GL/2022/15)" quando adotta nuove soluzioni di adeguata verifica a distanza o riveda quelle già in uso per l'onboarding di nuovi clienti.

Nel Regolamento Antiriciclaggio viene fornito il dettaglio relativo a:

- una descrizione generale delle soluzioni che la Banca ha posto in essere per raccogliere, verificare e conservare le informazioni nel corso di tutto il processo di onboarding a distanza del cliente, con la spiegazione delle caratteristiche e del funzionamento della soluzione;
- le situazioni in cui è possibile utilizzare la soluzione di onboarding a distanza del cliente, tenendo conto dei fattori di rischio individuati e valutati e dell'auto valutazione del rischio di riciclaggio e finanziamento del terrorismo connesso alla propria area di attività, compresa una descrizione della categoria di clienti, prodotti e servizi per i quali è ammissibile l'onboarding a distanza;
- le fasi che sono completamente automatizzate e quelle che richiedono l'intervento umano;
- i controlli in essere per assicurare che la prima operazione con un nuovo cliente sia eseguita solo dopo l'applicazione di tutte le misure di adeguata verifica iniziale della clientela.

Inoltre, ogniqualvolta venga valutata la possibilità di adottare una nuova soluzione per l'onboarding a distanza del cliente, la Banca effettua una valutazione preliminare all'attuazione di tale soluzione. Solo dopo avere accertato la possibilità di integrare tale soluzione nel proprio sistema di controlli interni, consentendo

così di gestire adeguatamente i rischi di riciclaggio e finanziamento del terrorismo che potrebbero derivare, la Banca inizia a utilizzare una nuova soluzione di onboarding a distanza del cliente.

3.1.4 RAPPORTI CONTINUATIVI E OPERAZIONI OCCASIONALI

La Banca procede all'adeguata verifica della clientela in relazione ai rapporti e alle operazioni che rientrano nella propria attività istituzionale, così come definita dalla normativa di settore.

Non è richiesta l'adeguata verifica per le attività finalizzate o connesse all'organizzazione, al funzionamento e all'amministrazione della Banca, tenuto conto che esse non rientrano nelle attività istituzionali e che, nel loro svolgimento, le controparti dei destinatari si configurano come prestatori di beni o servizi su iniziativa, piuttosto che come clienti che richiedono di instaurare un rapporto continuativo o di effettuare un'operazione occasionale (es., forniture per l'acquisizione di materiali o beni strumentali propri dell'impresa; acquisizione e manutenzione degli immobili ove viene esercitata l'attività istituzionale; prestazioni acquisite da liberi professionisti per consulenze).

3.2 PROFILATURA DELLA CLIENTELA

Il D.Lgs. 231/07 prevede che l'intensità e l'estensione degli obblighi di adeguata verifica della clientela siano modulati secondo il grado di rischio di riciclaggio associato al singolo cliente.

Le *Disposizioni su Adeguata Verifica* prevedono che la Banca definisca il *profilo di rischio* attribuibile a ogni cliente, sulla base dei complessivi elementi di valutazione e dei *fattori di rischio* ivi descritti (Sezione II e Allegati 1 e 2 delle *Disposizioni*). I diversi fattori di rischio vengono *ponderati* sulla base della loro importanza relativa. In esito alla profilatura, ciascun cliente è incluso in una delle *classi di rischio* predefinite dalla Banca.

3.2.1 SISTEMA DI PROFILATURA

La Banca elabora il profilo di rischio per ciascun cliente avvalendosi di algoritmi predefiniti, mediante procedura informatica, in grado di assegnare in automatico uno *scoring* sulla base delle informazioni raccolte mediante modulo di KYC. Dallo *scoring* assegnato al cliente viene derivata la *classe di rischio* (mediante associazione delle diverse classi di rischio ad intervalli di *scoring*).

Tale processo assicura che nel continuo lo *scoring* del cliente sia rideterminato tenendo conto dell'operatività realizzata e di eventuali fattori di rischio sopravvenuti. Il software intercetta nuovi elementi indicatori di maggiore o di minore rischio mediante analisi automatizzata dell'operatività del cliente e mediante raccolta di ulteriori fattori di rischio alimentati da fonti esterne, procedendo al ricalcolo dello *scoring* e, se necessario, all'aggiornamento del profilo di rischio.

Il meccanismo di ricalcolo o refresh del profilo di rischio assicura che i punteggi assegnati dagli algoritmi siano coerenti con l'evoluzione di contesto, dell'operatività del cliente e del quadro informativo complessivo. Tale processo viene eseguito mensilmente.

3.2.2 CALIBRAZIONE DELLE MISURE DI ADEGUATA VERIFICA IN BASE AL PROFILO DI RISCHIO

Le *Disposizioni su Adeguata Verifica* prevedono che a ciascuna classe di rischio è associato un coerente livello di profondità ed estensione delle misure adottate nell'adeguata verifica.

Di conseguenza, la Banca cura la gestione dei clienti con l'applicazione di:

- misure di Adeguata Verifica *semplificata* per i clienti a basso rischio, nei casi espressamente previsti dalla Policy;
- misure di Adeguata Verifica *rafforzata* in caso di clienti ad alto rischio, secondo schemi di lavoro tipici definiti dal D.Lgs. 231/07 e dalle *Disposizioni su Adeguata Verifica* emanate da Banca d'Italia (es. PEPs, paesi ad alto rischio);
- misure di Adeguata Verifica *ordinaria* in tutti gli altri casi.

L'associazione fra scoring - classe di rischio - profilo di rischio – misure di Adeguata Verifica viene sintetizzata nella tabella che segue:

	Classe 1	Classe 2	Classe 3	Classe 4
Denominazione	Basso	Medio Basso	Medio	Alto
Scoring	Da 1 a 5	Da 6 a 12	Da 13 a 24	Da 25 a 99
AV associata	Semplificata	Ordinaria	Ordinaria	Rafforzata

3.2.3 AGGIORNAMENTO DEL PROFILO DI RISCHIO

Come già accennato, la Banca ha il compito di verificare la congruità della classe di rischio assegnata al cliente al ricorrere di eventi o circostanze che sono suscettibili di modificare il profilo di rischio (es. nel caso di assunzione della qualifica di PEP, di cambiamenti rilevanti dell'operatività del cliente o della compagine societaria).

In relazione ai rapporti continuativi, la Banca definisce la frequenza ordinaria di aggiornamento della profilatura del cliente che deve risultare coerente con il livello di rischio.

Per il rinnovo dell'adeguata verifica sono definite le seguenti regole, che tengono conto del rischio assegnato al cliente :

- rischio basso, aggiornamento ogni 5 anni
- rischio medio basso, aggiornamento ogni 4 anni
- rischio medio, aggiornamento ogni 2 anni
- rischio alto, aggiornamento ogni anno.

Si dispone inoltre che l'adeguata verifica debba essere rinnovata, con aggiornamento del questionario, ogni qualvolta la Banca viene a conoscenza di:

- variazione dell'assetto societario (titolare effettivo, gruppo di appartenenza)
- variazione della forma giuridica, dell'oggetto sociale e/o del codice attività economica
- peggioramento del livello di rischio del cliente
- ripetuta comparsa di inattesi , sintomo di cambiamenti operativi o strutturali.

3.3 GESTIONE DEI FATTORI DI RISCHIO

La Banca applica misure di Adeguata Verifica proporzionali all'entità dei rischi di riciclaggio e di finanziamento del terrorismo. Le *Disposizioni su Adeguata Verifica* definiscono i criteri generali di valutazione del rischio, di seguito riportati.

Con riferimento ai criteri concernenti *il cliente*:

- devono considerare anche il titolare effettivo e, ove rilevante, l'esecutore;
- valutano l'ambito di attività e le caratteristiche del cliente, dell'eventuale titolare effettivo e, ove rilevante, dell'esecutore, nonché il paese o l'area geografica nei quali essi hanno la propria sede o la residenza o il domicilio o dai quali provengono i fondi; rilevano, inoltre, la localizzazione dell'attività svolta e i paesi con i quali il cliente o il titolare effettivo e, ove rilevante, l'esecutore hanno collegamenti significativi; l'importanza dei fattori di rischio legati al paese o all'area geografica varia in relazione alla tipologia di rapporto continuativo o di operazione;

- considerano il comportamento tenuto dal cliente o dall'esecutore al momento dell'apertura di rapporti continuativi ovvero del compimento di operazioni;
- nel caso di cliente diverso da una persona fisica, considerano le finalità della sua costituzione, gli scopi che persegue, le modalità attraverso cui opera per raggiungerli, nonché la forma giuridica adottata, soprattutto se essa presenti particolari elementi di complessità od opacità;
- verificano se il cliente e/o il titolare effettivo siano inclusi nelle "liste" delle persone e degli enti associati ad attività di finanziamento del terrorismo adottate dalla Commissione europea;

Con riferimento ai criteri concernenti *il rapporto o l'operazione*, per valutare il rischio di riciclaggio:

- considerano la struttura del prodotto o del servizio offerto, in termini di trasparenza e complessità e i canali attraverso cui esso è distribuito;
- nel valutare il rischio associato alla complessità del prodotto, del servizio o dell'operazione, considerano l'eventuale coinvolgimento di una pluralità di parti o di Paesi;
- prestano attenzione ai prodotti o servizi nuovi o innovativi, in particolare nel caso in cui, per l'offerta di questi prodotti o servizi, essi si avvalgano di nuove tecnologie o metodi di pagamento;
- considerano se il prodotto, servizio o operazione siano normalmente associati all'utilizzo di contante e se consentano operazioni di importo elevato;
- valutano la ragionevolezza del rapporto continuativo o dell'operazione in relazione all'attività svolta e al complessivo profilo economico del cliente e/o del titolare effettivo, tenendo conto di tutte le informazioni disponibili (es. la capacità reddituale e patrimoniale) e della natura e dello scopo del rapporto; in tale ambito possono effettuare valutazioni comparative con l'operatività di soggetti con similari caratteristiche professionali o dimensionali, di settore economico, di area geografica;
- valutano i canali di distribuzione e la fattispecie dell'Adeguata Verifica di terzi.

Di seguito vengono indicati i fattori di rischio considerati dalla Banca, fra gli altri, più rilevanti ai fini della profilatura.

3.3.1 FATTORI DI BASSO RISCHIO

3.3.1.1 FATTORI DI BASSO RISCHIO RELATIVI AL CLIENTE, ESECUTORE E TITOLARE EFFETTIVO

- Società ammesse alla quotazione su un mercato regolamentato, anche extra UE (specie se riconosciuto dalla Consob ai sensi dell'articolo 70 del TUF), e sottoposte ad obblighi di comunicazione che includono quelli di assicurare un'adeguata trasparenza della titolarità effettiva.
- Pubbliche amministrazioni ovvero istituzioni o organismi che svolgono funzioni pubbliche, conformemente al diritto dell'Unione europea
- Cliente o il titolare effettivo siano residenti, abbiano la sede principale delle proprie attività ovvero rilevanti collegamenti con paesi o aree geografiche a basso rischio (cfr nel seguito "fattori di basso rischio geografici").
- Intermediari bancari e finanziari elencati all'articolo 3, comma 2, del decreto antiriciclaggio - a eccezione di quelli di cui alle lettere i), o), s), v) - e intermediari bancari e finanziari comunitari o con sede in un paese terzo con un efficace regime di contrasto al riciclaggio e al finanziamento del terrorismo.

3.3.1.2 FATTORI DI BASSO RISCHIO RELATIVI A PRODOTTI, SERVIZI, OPERAZIONI O CANALI DI DISTRIBUZIONE

- Contratti di assicurazione vita rientranti nei rami indicati dall'articolo 2, comma 1, del decreto legislativo 7 settembre 2005, n. 209, quando il premio annuale non eccede 1.000 euro o il premio unico non è di importo superiore a 2.500 euro.
- Forme pensionistiche complementari disciplinate dal decreto legislativo 5 dicembre 2005, n. 252, se esse non prevedono clausole di riscatto diverse da quelle previste dall'articolo 14 del medesimo decreto e non possono servire da garanzia per un prestito al di fuori delle ipotesi previste dalla legge.
- Regimi di previdenza o sistemi analoghi che versano prestazioni pensionistiche ai dipendenti, in cui i contributi sono versati tramite detrazione dalla retribuzione e che non permettono ai beneficiari di trasferire i propri diritti.
- Prodotti o servizi finanziari che offrono servizi opportunamente definiti e circoscritti a determinate tipologie di clientela, volti a favorire l'inclusione finanziaria.
- Prodotti in cui i rischi di riciclaggio o di finanziamento del terrorismo sono mitigati da fattori, quali limiti di spesa o trasparenza della titolarità.

Rilevano in tale ambito prodotti con funzionalità limitate (es., con una soglia predeterminata di operatività o subordinati all'acquisto di uno specifico bene o servizio per il consumatore) e che non consentano l'anonimato o l'occultamento dell'identità del cliente e/o del titolare effettivo.

3.3.1.3 FATTORI DI BASSO RISCHIO GEOGRAFICI

- Paesi comunitari
- Paesi terzi dotati di efficaci sistemi di prevenzione del riciclaggio.
- Paesi terzi che fonti autorevoli e indipendenti valutano essere caratterizzati da un basso livello di corruzione o di permeabilità ad altre attività criminose.
- Paesi terzi che, sulla base di fonti autorevoli e indipendenti (es. rapporti di valutazione reciproca ovvero rapporti pubblici di valutazione dettagliata), siano dotati di un efficace sistema di prevenzione del riciclaggio e del finanziamento del terrorismo.

3.3.2 FATTORI DI RISCHIO ELEVATO

3.3.2.1 FATTORI DI RISCHIO ELEVATO RELATIVI AL CLIENTE, ESECUTORE E TITOLARE EFFETTIVO

- Rapporti continuativi o le operazioni occasionali con clienti e relativi titolari effettivi che rivestono la qualifica di persone politicamente esposte o PEP.
- Rapporti continuativi instaurati in circostanze anomale. A titolo esemplificativo, sono prese in considerazione circostanze in cui il cliente o l'esecutore sono riluttanti nel fornire le informazioni richieste, variano ripetutamente le informazioni fornite, danno informazioni incomplete o erranee o non sono in grado di produrre documentazione sulla propria identità, salvo i casi legittimi, quali quello dei richiedenti asilo. Sono tenuti in considerazione, altresì, eventuali comportamenti sintomatici della volontà del cliente di evitare l'instaurazione di un rapporto continuativo, ad esempio, quando il cliente chiede di effettuare una o più operazioni occasionali nonostante l'apertura di un rapporto continuativo risulterebbe economicamente più ragionevole.
- Rapporti continuativi, prestazioni professionali ed operazioni che coinvolgono Paesi Terzi ad Alto Rischio.
- Clienti e titolare effettivo residenti o aventi sede in aree geografiche a rischio elevato. Questo fattore ricorre quando il cliente o il titolare effettivo sono residenti o hanno la sede principale delle proprie attività ovvero rilevanti collegamenti con paesi a rischio elevato (cfr nel seguito "fattori di rischio elevato geografici").

- Clienti che pongono in essere operatività con aree geografiche a rischio elevato.
Clienti che pongono in essere operatività con controparti residenti o aventi sede in aree geografiche a rischio elevato (cfr nel seguito “fattori di rischio elevato geografici”).
- Indici reputazionali negativi relativi al cliente, al titolare effettivo e all’esecutore. Rileva la sussistenza di:
 - procedimenti penali (quando l’informazione è notoria o comunque nota alla Banca e non coperta da obblighi di segretezza che ne impediscono l’utilizzo) per fenomeni di riciclaggio o reati che possono essere reati presupposto di riciclaggio, quali reati fiscali, reati societari, reati fallimentari, corruzione, frode, associazione di tipo mafioso, associazione per delinquere;
 - procedimenti per danno erariale;
 - procedimenti per responsabilità amministrativa ex D.Lgs. 231/01;
 - sanzioni amministrative irrogate per violazione delle disposizioni antiriciclaggio a carico del cliente o del titolare effettivo;
 - misure cautelari o i provvedimenti di confisca circostanziati da parte delle Autorità e connessi a fenomeni riciclativi o reati che possono essere reati presupposto.

Tali fattori rilevano in quanto noti perché appresi da fonti informative esterne o perché la Banca è direttamente coinvolta con accessi o richieste delle Autorità. Nel valutare le notizie negative provenienti dai media o da altre fonti, la Banca ne considera la fondatezza e l’attendibilità basandosi sulla qualità e sull’indipendenza delle fonti informative e sulla ricorrenza delle informazioni.

- Invio alla UIF di segnalazione di operazioni sospette in relazione al cliente o al titolare effettivo.
- Ricorrenza di nominativi nelle liste delle persone o degli enti associati ai fini dell’applicazione degli obblighi di congelamento previsti dai Regolamenti comunitari o dai decreti adottati ai sensi del decreto legislativo 22 giugno 2007, n. 109.
- Strutture qualificabili come veicoli di interposizione patrimoniale. È il caso, a titolo esemplificativo, di trust, società fiduciarie e ulteriori soggetti giuridici che possono essere strutturati in maniera tale da beneficiare dell’anonimato e permettere rapporti con banche di comodo o con società aventi azionisti fiduciari.

Con riferimento alle società fiduciarie rilevano le fiduciarie di II livello che operano in conto proprio o che aprono rapporti per conto di fiducianti. Rilevano, altresì, i soggetti controllati direttamente o indirettamente da Fiduciarie/Trust o nella cui catena partecipativa giocano un ruolo chiave le Fiduciarie/Trust.

- Enti non profit;
- Tipo di attività economica caratterizzata da elevato utilizzo di contante. Rileva la riconducibilità delle attività economiche svolte dal cliente a tipologie particolarmente esposte ai rischi di riciclaggio quali il settore dei compro oro, di cambio valuta, del gioco o delle scommesse, attività prestata da agenti in attività finanziaria e “soggetti convenzionati e agenti” nel servizio di rimessa di denaro, money transfer.
- Tipo di attività economica riconducibile a settori particolarmente esposti a rischi di corruzione. Si tratta, in particolare, di settori economici interessati dall’erogazione di fondi pubblici, anche di origine comunitaria, appalti pubblici, sanità, edilizia, commercio di armi, difesa, industria bellica, industria estrattiva, raccolta e smaltimento dei rifiuti, produzione di energie rinnovabili.
- Cliente o titolare effettivo che ricoprono cariche pubbliche in ambiti non ricompresi dalla nozione di PEP ma per i quali comunque sussiste una rilevante esposizione al rischio di corruzione. Si fa

riferimento, ad esempio, agli amministratori locali, a soggetti con ruoli apicali nella pubblica amministrazione o in enti pubblici, consorzi e associazioni di natura pubblicistica.

- Soggetti con assetto proprietario anomalo o eccessivamente complesso data la natura dell'attività svolta; a tal fine occorre considerare la forma giuridica adottata dal cliente, specie ove presenti particolari elementi di complessità od opacità che impediscono o ostacolano l'individuazione del titolare effettivo o del reale oggetto sociale o di eventuali collegamenti azionari o finanziari con soggetti aventi sede in aree geografiche a rischio elevato.
- Clienti che abbiano aderito ad operazioni di regolarizzazione di patrimoni detenuti illecitamente all'estero, per il biennio successivo al compimento dell'operazione.

3.3.2.2 FATTORI DI RISCHIO ELEVATO RELATIVI A PRODOTTI, SERVIZI, OPERAZIONI O CANALI DI DISTRIBUZIONE

- Rapporti di corrispondenza transfrontalieri con un intermediario bancario o finanziario corrispondente con sede in un paese terzo.
- Servizi con un elevato grado di personalizzazione, offerti a una clientela dotata di un patrimonio di rilevante ammontare. Rilevano i servizi di gestione patrimoniale prestati a favore di clientela con elevate disponibilità economiche, specie se provenienti da settori economici ad alto rischio.
- Prodotti od operazioni che potrebbero favorire l'anonimato ovvero favorire l'occultamento dell'identità del cliente o del titolare effettivo. Rilevano, ad esempio, le carte prepagate anonime emesse da intermediari esteri, le azioni al portatore, le operazioni riconducibili a servizi connessi alla conversione di valuta legale in valuta virtuale e viceversa.
- Operazioni in contante frequenti e ingiustificate, caratterizzate dall'utilizzo di banconote in euro di grosso taglio ovvero dalla presenza di biglietti danneggiati o contraffatti.
- Operazioni di versamento di contante o valori provenienti dall'estero di importo complessivo pari o superiore al controvalore di 10.000 euro.
- Operazioni di relative a petrolio, armi, metalli preziosi, prodotti del tabacco, manufatti culturali e altri beni mobili di importanza archeologica, storica, culturale e religiosa o di raro valore scientifico, nonché avorio e specie protette.
- Utilizzo di piattaforme di scambio ovvero operazioni di acquisto/vendita pacchetti di moneta virtuale.
- Rapporti continuativi od operazioni occasionali a distanza non assistiti da adeguati meccanismi e procedure di riconoscimento.
- Pagamenti ricevuti da terzi privi di un evidente collegamento con il cliente o con la sua attività. Rilevano, a titolo esemplificativo, il pagamento di fatture effettuato da parte di terzi estranei al rapporto negoziale o triangolazioni di natura commerciale non supportate da idonea documentazione giustificativa, caratterizzate da pagamenti disposti da società estere prive di legami con l'intestatario della fattura, specie se con sede in aree geografiche a rischio elevato. Rientra in questo ambito, altresì, la ricezione di garanzie, specie se provenienti dall'estero e per importi rilevanti, da parte di terzi privi di collegamento con il cliente.
- Prodotti e pratiche commerciali di nuova generazione, che includono l'utilizzo di meccanismi di distribuzione o di tecnologie innovativi per prodotti nuovi o preesistenti.

3.3.2.3 FATTORI DI RISCHIO ELEVATO GEOGRAFICI

- Paesi terzi che fonti autorevoli e indipendenti ritengono carenti di efficaci presidi di prevenzione del riciclaggio.
- Paesi e aree geografiche valutati ad elevato livello di corruzione o di permeabilità ad altre attività criminose da fonti autorevoli e indipendenti.

- Paesi soggetti a sanzioni, embargo o misure analoghe adottate dai competenti organismi nazionali e internazionali.
- Paesi e aree geografiche che finanziano o sostengono attività terroristiche o nei quali operano organizzazioni terroristiche.
- Paesi valutati da fonti autorevoli e indipendenti come carenti sotto il profilo della conformità agli standard internazionali sulla trasparenza e lo scambio di informazioni a fini fiscali.

3.3.2.4 CLIENTI INDESIDERATI

In relazione ai fattori di rischio menzionati, è fatto divieto di accendere rapporti continuativi o accogliere la richiesta di operazioni da parte dei soggetti riconducibili alle seguenti categorie:

- soggetti che rifiutino di fornire informazioni necessarie per completare l'adeguata verifica sia per l'accensione del rapporto continuativo sia per il compimento di un'Operazione a rischio potenziale;
- soggetti che forniscano indicazioni sul titolare effettivo manifestamente discordanti da quanto emerge dalle fonti ufficiali (con l'intento di dare all'esterno un'immagine societaria difforme da quella fattuale).
- enti la cui società controllante abbia sede in Paesi terzi ad alto rischio.

Per le seguenti categorie di soggetti, in fase di allacciamento di nuove relazioni, è necessario avere l'autorizzazione del Direttore Generale, previo parere della Funzione Antiriciclaggio:

- soggetti già segnalati alla UIF;
- soggetti sottoposti a provvedimenti di tipo penale, o notoriamente indagati dall'A.G. con evidenza del dato dalle liste della W.C.L. o a mezzo stampa o altre fonti di pubblico accesso.

3.4 IDENTIFICAZIONE DEL TITOLARE EFFETTIVO

Il *titolare effettivo* è la persona fisica o le persone fisiche, diverse dal cliente, nell'interesse della quale o delle quali, in ultima istanza, il rapporto continuativo è istaurato, la prestazione professionale è resa o l'operazione è eseguita.

Il Gestore della relazione è il soggetto deputato, di norma, all'identificazione ed all'aggiornamento, tempo per tempo, dei dati relativi alla titolarità effettiva del Cliente, con contestuale aggiornamento del Questionario KYC.

L'identificazione del titolare effettivo ha luogo senza che sia necessaria la sua presenza fisica, contestualmente all'identificazione del cliente e sulla base dei dati identificativi da questi forniti. Si definisce che, in via ordinaria, le informazioni sul titolare effettivo siano richieste al cliente e da questi formalmente attestate e sottoscritte mediante Questionario KYC acquisendo nel caso di rapporti con clienti con profilo di rischio Alto, anche l'informazione sull'attività economica/professione svolta dal soggetto.

Il titolare effettivo di clienti diversi dalle persone fisiche coincide con la persona fisica o le persone fisiche cui, in ultima istanza, è attribuibile la proprietà diretta o indiretta dell'ente ovvero il relativo controllo.

Nel caso in cui il cliente sia una società di capitali:

- costituisce indicazione di proprietà diretta la titolarità di una partecipazione superiore al 25% del capitale del cliente, detenuta da una persona fisica;
- costituisce indicazione di proprietà indiretta la titolarità di una percentuale di partecipazioni superiore al 25% del capitale del cliente, posseduto per il tramite di società controllate, società fiduciarie o per interposta persona.

Nelle ipotesi in cui l'esame dell'assetto proprietario non consenta di individuare in maniera univoca la persona fisica o le persone fisiche cui è attribuibile la proprietà diretta o indiretta dell'ente, il titolare effettivo

coincide con la persona fisica o le persone fisiche cui, in ultima istanza, è attribuibile il controllo del medesimo in forza:

- del controllo della maggioranza dei voti esercitabili in assemblea ordinaria;
- del controllo di voti sufficienti per esercitare un'influenza dominante in assemblea ordinaria;
- dell'esistenza di particolari vincoli contrattuali che consentano di esercitare un'influenza dominante.

Qualora l'applicazione dei criteri precedenti non consenta di individuare univocamente uno o più titolari effettivi, il titolare effettivo coincide con la persona fisica o le persone fisiche titolari, conformemente ai rispettivi assetti organizzativi o statutari, di poteri di rappresentanza legale, amministrazione o direzione della società o del cliente comunque diverso dalla persona fisica.

Si ribadisce che, ai fini dell'individuazione del titolare effettivo, occorre fare riferimento alle informazioni rassegnate dal cliente e alle informazioni esterne reperite con la verifica di pubblici registri, elenchi, albi, atti o documenti conoscibili da chiunque. Il Gestore della relazione effettua il riscontro dei dati forniti dal cliente con informazioni desumibili da fonti affidabili e indipendenti, di cui acquisisce, in via autonoma o per il tramite del cliente, e conserva copie in formato cartaceo o elettronico.

Dovranno essere esaminati con molta cura i casi di difformità fra quanto dichiarato dal cliente in merito al titolare effettivo, e quanto invece risulta alla Banca da altre fonti (visure camerali, atti notarili etc); in tali circostanze, l'operatore dovrà prendere contatto con il Responsabile Antiriciclaggio per le valutazioni del caso (ad es. considerare l'inoltro della segnalazione di operazione sospetta, e la continuazione dell'eventuale rapporto continuativo). Ferme restando le prerogative del responsabile aziendale per le segnalazioni di operazioni sospette, nei casi sopra considerati, ed in tutte le ipotesi in cui si debba valutare l'opportunità di mantenere o meno la relazione, la decisione finale compete al Direttore Generale.

3.4.1 REGISTRO DEI TITOLARI EFFETTIVI

L'art. 21 del D.Lgs. 231/07 prevede che le imprese dotate di personalità giuridica tenute all'iscrizione nel Registro delle imprese e le persone giuridiche private tenute all'iscrizione nel Registro delle persone giuridiche private, hanno l'obbligo di comunicare le informazioni relative ai propri titolari effettivi, per via esclusivamente telematica e in esenzione da imposta di bollo, al Registro delle imprese, ai fini della conservazione in apposita sezione ad accesso riservato.

Tale norma, in corso di attuazione, prevede che, a tendere, la Sezione dei Titolari Effettivi del Registro delle Imprese possa essere considerata quale fonte utile per verificare le informazioni sul titolare effettivo fornite dal cliente.

La Banca intende adottare gli adeguati presidi affinché, non appena disponibile il registro dei titolari effettivi, tale informazione venga utilizzata nel processo di adeguata verifica della Clientela.

3.5 CONTROLLO COSTANTE E TRANSACTION MONITORING

La Banca assicura il controllo costante nel corso del rapporto continuativo attraverso il monitoraggio delle operazioni effettuate dalla clientela, al fine di verificarne la coerenza con le informazioni acquisite nell'ambito dell'adeguata verifica della clientela, con il profilo economico-finanziario del cliente e con il relativo livello di rischio di riciclaggio e di finanziamento del terrorismo.

Il monitoraggio è finalizzato ad individuare operazioni che, per caratteristiche, entità, frequenza, modalità di esecuzione o area geografica di riferimento, possano risultare incoerenti rispetto al profilo del cliente o presentare elementi di potenziale anomalia, anche con riguardo, ove necessario, all'origine dei fondi e alla finalità economica delle operazioni.

A tal fine la Banca si avvale di un sistema informatico di Transaction Monitoring, che analizza l'operatività della clientela sulla base di specifici indicatori di anomalia e parametri di rischio, generando segnalazioni di operatività potenzialmente anomala (*alert*).

Gli *alert* generati dal sistema sono sottoposti ad analisi da parte dei Controlli di primo livello, che verificano la coerenza dell'operatività rispetto al quadro conoscitivo acquisito e segnalando tempestivamente alla Funzione Antiriciclaggio eventuali operazioni ritenute inattese o incoerenti con il profilo del cliente.

Le attività di monitoraggio tengono conto, tra l'altro, di operatività caratterizzate da elementi di rischio quali, a titolo esemplificativo:

- operazioni di importo rilevante o caratterizzate da frazionamento;
- operazioni incoerenti con il profilo economico-finanziario del cliente;
- operazioni con controparti o verso/da Paesi a rischio di riciclaggio o finanziamento del terrorismo;
- utilizzo anomalo di contante.

Gli esiti delle attività di monitoraggio sono utilizzati anche ai fini dell'aggiornamento del profilo di rischio della clientela e della valutazione, ove ne ricorrano i presupposti, dell'eventuale inoltro di Segnalazioni di Operazioni Sospette, secondo quanto previsto dalla normativa vigente e dalle procedure interne della Banca.

3.6 ADEGUATA VERIFICA ORDINARIA

La Banca è destinataria degli obblighi di adeguata verifica previsti dal D.Lgs. 231/2007 e dalle successive disposizioni in materia di antiriciclaggio e contrasto al finanziamento del terrorismo.

L'adeguata verifica ordinaria si applica a tutti i clienti nei casi in cui non ricorrano condizioni di basso rischio, tali da consentire l'applicazione di misure semplificate, né situazioni di rischio elevato che richiedano misure rafforzate.

Le principali attività di adeguata verifica ordinaria comprendono:

- Identificazione e verifica dell'identità del cliente e del titolare effettivo, mediante acquisizione di documenti ufficiali e informazioni affidabili, indipendenti e aggiornate, in conformità agli artt. 17-19 del D.Lgs. 231/2007.
- Raccolta di informazioni sul cliente, incluse natura, scopo e tipologia delle operazioni previste o abituali, al fine di consentire una corretta valutazione del profilo di rischio e la classificazione del cliente.
- Valutazione del profilo di rischio, considerando fattori quali origine dei fondi, attività economica o professionale, collocazione geografica, tipologia di operazioni e comportamenti transazionali.
- Controllo costante del rapporto continuativo, attraverso il monitoraggio periodico delle operazioni effettuate, in coerenza con le informazioni acquisite e il profilo di rischio del cliente, anche mediante strumenti automatizzati di Transaction Monitoring.
- Aggiornamento periodico dei dati e dei documenti del cliente, secondo la frequenza determinata dal rischio complessivo del rapporto e dalle procedure interne della Banca, garantendo la conformità alla normativa vigente e alla Policy interna.

L'Adeguata Verifica Ordinaria rappresenta la base obbligatoria per tutte le relazioni continuative, sulla quale si innestano eventuali misure di Adeguata Verifica Semplificata o Rafforzata, assicurando un presidio proporzionato e coerente del rischio di riciclaggio e finanziamento del terrorismo, in linea con gli artt. 16 e seguenti del D.Lgs. 231/2007 e con le disposizioni di Banca d'Italia in materia di controllo interno e Transaction Monitoring.

3.7 ADEGUATA VERIFICA SEMPLIFICATA

Le misure di Adeguata Verifica Semplificata sono applicate nei casi in cui, a seguito della valutazione effettuata dalla Banca secondo l'approccio basato sul rischio, il rapporto o l'operazione presentino un livello di rischio di riciclaggio e di finanziamento del terrorismo basso.

In tale ambito, la Banca può applicare misure semplificate, tra l'altro, nei confronti delle seguenti categorie di clienti, purché sia confermata in concreto la sussistenza di un basso rischio:

- società ammesse alla quotazione su mercati regolamentati e sottoposte ad obblighi di trasparenza sulla titolarità effettiva;
- pubbliche amministrazioni o organismi che svolgono funzioni pubbliche conformemente al diritto dell'Unione europea, fermo restando che tale regime non si estende automaticamente agli enti partecipati o controllati;
- intermediari bancari e finanziari soggetti a obblighi equivalenti in materia antiriciclaggio.

Nel valutare la sussistenza del basso rischio, la Banca tiene conto anche di eventuali elementi negativi, quali l'applicazione di sanzioni o misure di vigilanza per violazioni in materia antiriciclaggio.

Le misure semplificate non trovano applicazione o cessano di essere applicate qualora:

- vengano meno le condizioni di basso rischio;
- emergano elementi di incoerenza nell'operatività del cliente;
- sussista il sospetto di riciclaggio o finanziamento del terrorismo.

L'identificazione del titolare effettivo può essere effettuata anche mediante dichiarazione del cliente, fermo restando l'obbligo e la responsabilità della Banca di verificarne la coerenza e la plausibilità sulla base delle informazioni disponibili.

La frequenza di aggiornamento del Questionario KYC, cioè dei dati raccolti ai fini dell'adeguata verifica semplificata, è fissata a 5 anni.

3.8 ADEGUATA VERIFICA RAFFORZATA

La normativa dispone di applicare misure rafforzate di adeguata verifica della clientela quando sussiste un elevato rischio di riciclaggio, risultante da specifiche previsioni normative ovvero dall'autonoma valutazione dell'impresa.

Si considerano *sempre* a rischio elevato:

- i rapporti continuativi, prestazioni professionali ed operazioni che coinvolgono paesi terzi ad alto rischio;
- i rapporti di corrispondenza transfrontalieri con un intermediario bancario o finanziario rispondente con sede in un Paese terzo o che comportano l'esecuzione di servizi per le crypto-attività con un intermediario bancario o finanziario, corrispondente di un Paese terzo;
- rapporti continuativi, prestazioni professionali o operazioni con clienti e relativi titolari effettivi che siano persone politicamente esposte (PEP), salve le ipotesi in cui le predette persone politicamente esposte agiscono in veste di organi delle pubbliche amministrazioni.

Per le suddette fattispecie di rischio elevato è necessaria l'autorizzazione del Direttore Generale all'avvio o prosecuzione del rapporto o al compimento dell'operazione occasionale, il quale si esprime previo parere della Funzione AML. Qualora il Direttore Generale decida di non adeguarsi al parere rilasciato dalla Funzione Antiriciclaggio, è tenuto a formalizzare e motivare la decisione e a individuare le misure che devono essere adottate per mitigare i rischi segnalati.

Inoltre, nell'applicazione di misure rafforzate di adeguata verifica della clientela, la Banca tiene conto, almeno, dei seguenti fattori:

a) fattori di rischio relativi al cliente quali:

- rapporti continuativi o prestazioni professionali instaurati ovvero eseguiti in circostanze anomale;
- clienti residenti o aventi sede in aree geografiche ad alto rischio secondo i criteri di cui alla lettera c);
- strutture qualificabili come veicoli di interposizione patrimoniale;
- società che hanno emesso azioni al portatore o siano partecipate da fiduciari;
- tipo di attività economiche caratterizzate da elevato utilizzo di contante;
- assetto proprietario della società cliente anomalo o eccessivamente complesso data la natura dell'attività svolta;

b) fattori di rischio relativi a prodotti, servizi, operazioni o canali di distribuzione quali:

- servizi con un elevato grado di personalizzazione, offerti a una clientela dotata di un patrimonio di rilevante ammontare;
- prodotti od operazioni che potrebbero favorire l'anonimato;
- rapporti continuativi, prestazioni professionali od operazioni occasionali a distanza, non assistiti da procedure di identificazione elettronica sicure e regolamentate ovvero autorizzate o riconosciute dall'Agenzia per l'Italia digitale;;
- pagamenti ricevuti da terzi privi di un evidente collegamento con il cliente o con la sua attività
- prodotti e pratiche commerciali di nuova generazione, compresi i meccanismi innovativi di distribuzione e l'uso di tecnologie innovative o in evoluzione per prodotti nuovi o preesistenti
- operazioni relative a petrolio, armi, metalli preziosi, prodotti del tabacco, manufatti culturali e altri beni mobili di importanza archeologica, storica, culturale e religiosa o di raro valore scientifico, nonché avorio e specie protette

c) fattori di rischio geografici quali quelli relativi a:

- Paesi terzi che, sulla base di fonti attendibili e indipendenti quali valutazioni reciproche ovvero rapporti pubblici di valutazione dettagliata, siano ritenuti carenti di efficaci presidi di prevenzione del riciclaggio e del finanziamento del terrorismo coerenti con le raccomandazioni del GAFI;
- Paesi terzi che fonti autorevoli e indipendenti valutano essere caratterizzati da un elevato livello di corruzione o di permeabilità ad altre attività criminose;
- Paesi soggetti a sanzioni, embargo o misure analoghe emanate dai competenti organismi nazionali e internazionali;
- Paesi che finanziano o sostengono attività terroristiche o nei quali operano organizzazioni terroristiche.

Le misure di adeguata verifica rafforzata si sostanziano nell'acquisizione di maggiori informazioni sul cliente e sull'eventuale titolare effettivo. in una più accurata valutazione della natura e dello scopo del rapporto, nell'intensificazione della frequenza delle verifiche e in una maggiore profondità delle analisi effettuate nell'ambito dell'attività di controllo costante del rapporto continuativo. Per maggiore dettaglio sulle procedure di adeguata verifica rafforzata si rimanda a quanto riportato nel Regolamento Antiriciclaggio.

3.9 PERSONE POLITICAMENTE ESPOSTE

Il D.Lgs. 231/07 definisce le Persone Politicamente Esposte (PPE o PEP Political Exposure Persons) le persone fisiche che occupano o hanno cessato di occupare da meno di un anno importanti cariche pubbliche, nonché i loro familiari e coloro che con i predetti soggetti intrattengono notoriamente stretti legami.

Tutti questi soggetti rivestono la qualità di PEP e sono classificati in classe di rischio Alto e gestiti con procedure di adeguata verifica rafforzata.

Inoltre, la Banca prevede che i seguenti soggetti:

- delegati della PEP;
- soggetti che hanno delegato la PEP;
- cointestatari di rapporti continuativi;
- società di appartenenza qualora la PEP sia legale rappresentante, titolare effettivo o socio;
- titolari effettivi della società di appartenenza della PEP;
- soggetti notoriamente collegati alla PEP;

debbano ereditare, di norma, il profilo di rischio Alto dalla PEP.

Per l'individuazione delle PEP la Banca utilizza provider esterni in grado di garantire un costante aggiornamento delle informazioni. Oltre a ciò, in fase di instaurazione del rapporto, vengono utilizzate tutte le informazioni disponibili a livello aziendale ed extra aziendale. Il Gestore della relazione è obbligato a raccogliere tutte le informazioni rilevanti, anche di tipo informale, facendo leva sulla collaborazione del cliente PEP nel fornire dati utili sulla propria posizione e per disegnare la rete di relazioni familiari e di affari. Inoltre, il Gestore della relazione deve far leva nell'utilizzo delle eventuali informazioni raccolte in fase di istruttoria per la concessione di finanziamenti o il questionario MiFID ovvero le eventuali informazioni desunte da fonti esterne aperte (notizie giornalistiche attendibili su stampa o internet).

Si dispone che dopo l'esecuzione delle fasi del processo di Adeguata Verifica rafforzata, il Gestore della relazione, che abbia formulato parere positivo nella scheda di Adeguata Verifica Rafforzata, deve dare corso al *processo di escalation* richiedendo autorizzazione per l'avvio del rapporto continuativo o per l'esecuzione dell'operazione occasionale al Direttore Generale. Quest'ultimo si esprime previo parere della Funzione AML; qualora decida di non adeguarsi al parere rilasciato dalla Funzione AML, è tenuto a formalizzare e motivare la decisione e a individuare le misure che devono essere adottate per mitigare i rischi segnalati.

L'iter autorizzativo si svolge su tre livelli di istruttoria che coinvolge:

- il Titolare di Filiale;
- la Funzione AML, che rilascia un *parere* sull'avvio del rapporto o sull'esecuzione dell'operazione occasionale dopo aver valutato la correttezza e la completezza dell'Adeguata Verifica rafforzata svolta e dopo aver eseguito, se necessario, le proprie verifiche (es. su liste esterne e interne, su liste crime, sui media, su indicatori reputazionali e ragionevole certezza della liceità dei fondi);
- il Direttore Generale, per il rilascio dell'autorizzazione all'avvio del rapporto o all'esecuzione, che si avvale del parere formulato dalla Funzione AML.

3.10 RAPPORTI DI CORRISPONDENZA CON INTERMEDIARIO DI PAESE TERZO EXTRA UE

L'art. 25 del D.Lgs. 231/07 dispone che nel caso di rapporti di corrispondenza transfrontalieri con un ente creditizio o istituto finanziario corrispondente di un paese terzo extra UE gli intermediari bancari e finanziari, oltre alle ordinarie misure di adeguata verifica della clientela, adottano ulteriori misure rafforzate.

La Banca si astiene dall'accensione di rapporti continuativi con enti corrispondenti di stati extracomunitari (il mero scambio di chiavi SWIFT non determina l'apertura di un rapporto di corrispondenza).

3.11 ASTENSIONE

Ai sensi della normativa vigente, quando la Banca non è in grado di rispettare gli obblighi di adeguata verifica della clientela non può instaurare il rapporto continuativo.

Ai sensi dell'articolo 42 c. 2 del D.Lgs. 231/07, vi è l'obbligo di astensione dall'instaurare o proseguire rapporti continuativi o eseguire operazioni di cui siano parte, direttamente o indirettamente, società fiduciarie, *trust*, società anonime (o controllate attraverso azioni al portatore) con sede in Paesi terzi ad alto rischio.

Sempre ai sensi dell'art. 42 c. 2 del D.Lgs. 231/07, vi è l'obbligo di astensione dall'instaurare o proseguire rapporti continuativi o eseguire operazioni di cui siano, direttamente o indirettamente parte entità giuridiche, altrimenti denominate, aventi sede nei suddetti Paesi, di cui non è possibile identificare il titolare effettivo né verificarne l'identità.

In ogni caso, al ricorrere delle fattispecie menzionate, la Banca valuta se effettuare una segnalazione di operazione sospetta.

3.12 DE-RISKING

Ferme restando l'obbligo di astensione di cui all'art. 42 del Decreto, qualora la Banca intenda adottare la decisione di rifiutare ovvero interrompere un Rapporto Continuativo o astenersi dal compiere un'Operazione si accerta di aver preso in considerazione ed escluso tutte le possibili misure di mitigazione ragionevolmente applicabili alla fattispecie, tenendo conto del rischio di riciclaggio associato al Rapporto Continuativo esistente o potenziale o all'Operazione.

La Banca utilizza le informazioni riguardanti la propria Clientela e le operazioni da essa svolte, acquisite nel quadro delle procedure di adeguata verifica, al fine di valutare se le transazioni e i rapporti siano riconducibili - in maniera diretta o indiretta - a soggetti o entità coinvolti in attività di riciclaggio o di finanziamento del terrorismo, ovvero in programmi di sviluppo di armi di distruzione di massa, non supportando in alcun modo operazioni che riguardino armi controverse e/o bandite dai trattati internazionali, ad esempio armi nucleari, biologiche e chimiche, bombe a grappolo, armi contenenti uranio impoverito, mine terrestri antipersona. Con riferimento alla produzione, al transito e/o alla commercializzazione di materiali di armamento diversi da quelli sopra indicati, il Gruppo può supportare le operazioni che abbiano ricevuto autorizzazione da parte delle autorità di competenza e che siano conformi alla legislazione applicabile e vigente nel comparto.

Inoltre, la Banca si astiene dall'instaurare o mantenere relazioni d'affari con soggetti particolarmente esposti al rischio di riciclaggio/finanziamento del terrorismo quali:

- clienti per i quali la Banca si è trovata nell'impossibilità oggettiva di effettuare l'adeguata verifica della clientela, ai sensi dell'art. 42, co. 1 del Decreto Antiriciclaggio;
- case di gioco e scommesse, anche on line, società dedite all'esercizio del gioco del "Bingo", per i quali non risultino rilasciate e verificabili le autorizzazioni e/o concessioni previste dalla normativa vigente da almeno 3 anni.
- soggetti convenzionati e agenti di prestatori di servizi di pagamento (di cui alla definizione dell'art. 1 c. 2 lettera nn), istituti di moneta elettronica e money transfert che non siano rispondenti a quanto previsto dal Capo V del D.Lgs. 231/07 agli art. 43 e seguenti;
- clientela presente in liste antiterrorismo.

3.13 ESECUZIONE DELL'ADEGUATA VERIFICA DA PARTE DI TERZI

La Banca può commercializzare prodotti e servizi per il tramite di terzi e demandare a questi, in tutto o in parte, l'assolvimento degli adempimenti di adeguata verifica della clientela – ad eccezione del controllo costante – ferma la piena responsabilità della Banca per l'osservanza di detti obblighi.

Il ricorso ai terzi è consentito dal Decreto Antiriciclaggio per tutte le fasi dell'adeguata verifica, ad eccezione del controllo costante dell'operatività (identificazione del cliente e del titolare effettivo, verifica dei dati

relativi ai medesimi, acquisizione di informazioni sullo scopo e la natura del rapporto e delle operazioni). La Banca può decidere di avvalersi delle verifiche condotte da un terzo (a condizione che sussistono i presupposti previsti dal Decreto Antiriciclaggio per avvalersi della verifica della clientela condotta da terzi) qualora:

- in base alle informazioni raccolte il rischio di riciclaggio e di finanziamento al terrorismo risulti “basso” ovvero “medio basso”;
- sia accertato che le misure di adeguata verifica applicate dal terzo presuppongono una valutazione del rischio di riciclaggio e di finanziamento al terrorismo omogenea rispetto a quella condotta dalla Banca;
- non vi siano motivi per dubitare della corretta esecuzione delle verifiche da parte del terzo.

La Banca tiene traccia documentale delle valutazioni e verifiche di cui sopra.

L’attestazione deve essere riconducibile al terzo attestante, attraverso accorgimenti idonei (sottoscrizione cartacea da parte del personale a ciò autorizzato, invio con sistemi informatici, ecc.) e deve essere trasmessa dal terzo attestante e non dal Cliente.

L’attestazione deve espressamente confermare il corretto adempimento degli obblighi antiriciclaggio da parte dell’attestante, in relazione alle varie attività effettuate. Il contenuto dell’attestazione varia a seconda dello specifico obbligo di adeguata verifica cui essa è diretta; in base a tale criterio, essa deve contenere:

- i dati identificativi del cliente, dell’esecutore e del titolare effettivo ai fini dell’adempimento dell’obbligo di identificazione;
- l’indicazione delle tipologie delle fonti utilizzate per l’accertamento e per la verifica dell’identità del Cliente e del Titolare effettivo;
- le informazioni sulla natura e sullo scopo del rapporto continuativo da aprire e dell’operazione occasionale da eseguire ai fini dell’adempimento del relativo obbligo.

In ogni caso, la Banca valuta se gli elementi raccolti e le verifiche effettuate dai terzi siano aggiornati, idonei e sufficienti per l’assolvimento degli obblighi di adeguata verifica e, qualora non li reputi tali, provvederà a informare il terzo delle eventuali carenze, incongruità riscontrate.

La Banca adempie in via diretta agli obblighi di adeguata verifica o si astiene dall’instaurare il rapporto o dall’eseguire l’operazione, valutando se effettuare una SOS, qualora ricorrano i presupposti. Nell’ambito delle modalità di raccolta e di scambio delle informazioni, nella commercializzazione di prodotti e servizi per il tramite di terzi la Banca provvede a:

- definire con il terzo le fasi dell’adeguata verifica demandate, individuando i dati e le informazioni da trasmettere, le modalità e la tempistica;
- definire le modalità e gli strumenti per lo scambio tempestivo dei flussi informativi
- verificare, nei limiti della diligenza professionale, la veridicità dei documenti ricevuti e la correttezza e attendibilità delle informazioni desunte dagli stessi
- acquisire, ove necessario, informazioni supplementari dai terzi, dal cliente, da altre fonti pubbliche.

È fatto comunque divieto di avvalersi, per l’esecuzione delle attività di adeguata verifica della clientela, di terzi aventi sede in Paesi Terzi ad Alto rischio.

3.14 ESECUZIONE DELL’ADEGUATA VERIFICA SUI FORNITORI

La Banca, nell’ambito della propria attività di prevenzione del riciclaggio e del finanziamento del terrorismo, si assicura che i fornitori terzi siano sottoposti ad un’analisi preventiva e periodica finalizzata a verificarne, in concreto, il rischio di riciclaggio e finanziamento al terrorismo.

3.15 CONTROLLI IN MATERIA DI ANTITERRORISMO ED EMBARGHI INTERNAZIONALI E SUL TRASFERIMENTO DI FONDI

In considerazione della crescente rilevanza assunta dalla lotta al terrorismo internazionale, ai programmi di sviluppo delle armi di distruzione di massa e al commercio di prodotti e tecnologie a duplice uso ("dual use"), la Banca adotta procedure interne di controllo in grado di identificare quei clienti o quelle transazioni che presentino un elevato rischio di coinvolgimento in attività, di natura commerciale o finanziaria, poste in essere dalla clientela in violazione di provvedimenti restrittivi adottati dalla comunità internazionale nei confronti di determinati Paesi, persone fisiche e giuridiche, entità, organizzazioni.

Tali controlli, complementari a quelli svolti nell'ambito delle ordinarie procedure di adeguata verifica, possono suddividersi in:

- 1) controlli sui nominativi: si applicano ai nominativi controparti nelle movimentazioni di fondi, allo scopo di accertare che la clientela non operi con soggetti destinatari di sanzioni emanate da organismi internazionali comportanti l'obbligo di congelamento dei fondi e delle risorse economiche, ovvero l'applicazione di misure restrittive di diversa natura (cosiddetti «soggetti designati»). In tale contesto, vengono considerate le liste delle persone e delle entità soggette a misure restrittive applicate da Unione Europea, ONU, OFAC e SECO (Segreteria di Stato dell'Economia, Svizzera);
- 2) controlli sul Paese: si applicano ai Paesi di provenienza e/o conduzione degli affari dei soggetti clienti, nonché ai Paesi di origine e destinazione dei fondi dagli stessi movimentati, con l'obiettivo di verificarne l'appartenenza al novero dei Paesi o territori a rischio;
- 3) destinatari di embarghi internazionali per scarso contrasto all'attività terroristica o violazione di diritti umani fondamentali; controlli transazionali: si applicano all'operatività di trasferimento dei fondi effettuata dalla clientela e agli eventuali beni o servizi ad essa sottostanti, per verificare che non siano violati provvedimenti di embargo o analoghe restrizioni di natura commerciale (a esempio divieti o limitazioni all'import/export di merci, materie prime e tecnologie) o finanziaria (a esempio divieti o restrizioni ai servizi finanziari, agli investimenti, alle transazioni di capitali).

Quale risultanza dei controlli svolti, ove siano identificate situazioni a rischio elevato, vengono attivate misure di tipo rafforzato volte ad acquisire dati e informazioni supplementari, anche mediante la produzione di idonea documentazione, e a monitorare con particolare intensità l'evoluzione dei rapporti facenti capo al soggetto, fermo restando l'obbligo di procedere alla segnalazione di operazioni sospette quando ne sussistano le condizioni.

Nelle specifiche circostanze indicate dalle norme nazionali e comunitarie in materia di embarghi vengono inoltre ottemperati gli adempimenti di congelamento dei fondi e delle risorse economiche spettanti alle persone o entità interessate dalle misure restrittive, e con essi il divieto di mettere a loro disposizione capitali o risorse economiche. Sono altresì attivate le procedure di notifica, comunicazione o richiesta di autorizzazione alle competenti Autorità eventualmente previste dai provvedimenti sanzionatori.

Infine, nel rispetto di quanto previsto dal Regolamento (UE) 2015/847 del Parlamento Europeo e del Consiglio del 20 maggio 2015 riguardante i dati informativi che accompagnano i trasferimenti di fondi, la Banca adotta procedure in grado di individuare le informazioni sull'ordinante e sul beneficiario che devono essere contenute nei trasferimenti di fondi.

4 CONSERVAZIONE E SEGNALAZIONE

4.1 CONSERVAZIONE DEI DOCUMENTI E DEI DATI

4.1.1 CONSERVAZIONE DEI DOCUMENTI

La Banca conserva i documenti acquisiti nell'effettuazione dell'adeguata verifica, incluse le scritture e le registrazioni delle operazioni, in originale ovvero in copia avente efficacia probatoria ai sensi della normativa vigente.

I documenti sono conservati per un periodo di dieci anni decorrenti dalla data di esecuzione dell'operazione occasionale ovvero di chiusura del rapporto continuativo. I documenti sono prontamente disponibili, di norma in formato elettronico, su richiesta delle Autorità.

Per approfondimenti tecnici si rimanda alle *Disposizioni per la conservazione dei dati e delle informazioni* emanato da Banca d'Italia.

4.1.2 CONSERVAZIONE DEI DATI

La Banca garantisce che gli archivi informatizzati e le procedure adottati per la conservazione e l'utilizzo dei dati e delle informazioni relativi ai clienti soddisfino le specifiche previsioni contenute nel D. Lgs. 231/07, nonché nelle *Disposizioni per la conservazione dei dati e delle informazioni* emanato da Banca d'Italia.

Per la conservazione dei dati e delle informazioni, la Banca si avvale di un Archivio Unico Informatico (AUI) tenuto in conformità delle normative vigenti. Dunque, al fine di assolvere l'obbligo di conservazione, in linea di continuità con il precedente regime di registrazione dei dati e delle informazioni che prevedevano l'istituzione di un Archivio Unico Informatico, la Banca continua ad avvalersi dello stesso.

Le registrazioni in AUI vengono alimentate attraverso specifici flussi informativi contenenti le informazioni ed i dati richiesti per la corretta alimentazione dello stesso.

Per quanto attiene le modalità di conservazione dei dati, la Funzione AML ha la responsabilità di verificare l'accessibilità completa e tempestiva ai dati a fronte di ispezioni o richieste da parte delle Autorità nonché l'acquisizione della totalità dei dati minimi richiesti dalla normativa entro 30 giorni dall'instaurazione, variazione o chiusura del rapporto continuativo o dall'esecuzione dell'operazione.

4.2 OBBLIGHI DI COMUNICAZIONE

4.2.1 FLUSSO SARA

La Banca è tenuta a trasmettere alla UIF con cadenza periodica, i dati concernenti la propria operatività per consentire alla stessa di svolgere le analisi finalizzate all'individuazione di eventuali fenomeni di riciclaggio o di finanziamento del terrorismo. A tal fine, per quanto attiene alle *Segnalazioni antiriciclaggio aggregate S.Ar.A di cui al Provvedimento UIF del 2014*, la Banca invia mensilmente flussi contenenti le operazioni registrate in AUI nel periodo di riferimento;

L'invio dei dati, aggregati secondo quanto previsto dal detto Provvedimento, deve essere effettuato entro il 2° giorno del 3° mese successivo a quello di riferimento delle operazioni.

La Funzione antiriciclaggio è Responsabile dell'invio delle *Segnalazioni antiriciclaggio aggregate S.Ar.A*.

4.2.2 COMUNICAZIONI OGGETTIVE

La Banca trasmette all'UIF, con cadenza mensile, una comunicazione c.d. "Comunicazioni oggettive", contenente ogni operazione, anche occasionale, di movimentazione di denaro contante di importo pari o superiore a 10.000 euro eseguita nel corso del mese solare, anche se realizzata attraverso più operazioni singolarmente pari o superiori a 1.000 euro da parte dello stesso cliente o esecutore.

L'inclusione dell'operazione nella comunicazione oggettiva esclude l'obbligo di segnalazione dell'operazione come sospetta ai sensi dell'art. 35 del d. lgs. 231/2007 qualora la stessa:

- *non presenti collegamenti con altre operazioni di diversa tipologia che facciano desumere una complessiva operatività sospetta*

- *non sia effettuata da clienti a elevato rischio di riciclaggio e finanziamento del terrorismo (clienti con profilo di rischio “Alto”)*

In ogni caso l’inoltro di una segnalazione di operazione sospetta non esonera dall’invio della comunicazione oggettiva sull’operazione.

Le operazioni, trasmesse secondo lo schema segnaletico di cui alle *Istruzioni in materia di Comunicazioni oggettive* emanate da UIF vengono inviate dal Responsabile della Funzione AML entro il 15° giorno lavorativo del 2° mese successivo a quello di riferimento.

Il Responsabile della Funzione, che può abilitare altri soggetti all’inserimento e trasmissione delle comunicazioni oggettive rappresenta l’interlocutore della UIF.

5 PRESI SU PRODOTTI ASSICURATIVI, SERVIZI DI PAGAMENTO E STRUMENTI DIGITALI

5.1 PRESIDI SULLA DISTRIBUZIONE DI PRODOTTI ASSICURATIVI DA PARTE DELLA BANCA

L’art. 20 del Reg. 44 emanato da IVASS prevede che le imprese assicurative “adottano ogni precauzione necessaria ad assicurare il rispetto delle disposizioni in materia di prevenzione del rischio di riciclaggio e di finanziamento al terrorismo nella vendita di prodotti assicurativi tramite rete distributiva diretta”.

Le Compagnie assicurative commercializzano i propri prodotti, principalmente, per il tramite di una rete distributiva diretta, di cui possono far parte banche, cui è demandato l’assolvimento degli adempimenti di adeguata verifica della clientela.

La Banca distribuisce prodotti assicurativi per le Compagnie, con le quali stipula Accordi di distribuzione, contenenti specifiche clausole finalizzate ad assicurare il rispetto delle disposizioni in materia di prevenzione del rischio di riciclaggio e di finanziamento del terrorismo nella commercializzazione dei prodotti assicurativi.

La distribuzione dei prodotti assicurativi è riservata esclusivamente alla clientela della Banca titolare di un conto corrente e di un dossier titoli. Tale presidio consente alla Banca di operare nell’ambito di rapporti già oggetto di adeguata verifica della clientela, assicurando il rispetto delle normative vigenti in materia di prevenzione del riciclaggio e del finanziamento del terrorismo.

Tali clausole richiamano, in particolare, le regole di comportamento a cui debbono attenersi le unità operative della Banca in quanto soggetto collocatore che compone la rete distributiva diretta della Compagnia in tema di:

- adeguata verifica;
- procedura PEP;
- procedura SOS;
- formazione degli addetti;
- dati e informazioni da acquisire in fase di apertura del rapporto ai fini dell’adeguata verifica.

Inoltre, in sede di collocamento di un prodotto assicurativo, viene comunque compilato uno specifico questionario informativo e di adeguata verifica predisposto dalla singola Compagnia assicurativa, al fine di raccogliere e aggiornare le informazioni richieste dalla normativa e dalle procedure interne della Compagnia stessa.

5.2 PRESIDI IN MATERIA DI SERVIZI DI PAGAMENTO E DI STRUMENTI DIGITALI

La Banca, nell'ambito dell'offerta di servizi di pagamento e strumenti digitali (quali carte di pagamento, strumenti di moneta elettronica etc.), adotta specifici presidi volti a prevenire e mitigare i rischi di riciclaggio e di finanziamento del terrorismo, in coerenza con la normativa vigente e con l'approccio basato sul rischio.

Tali strumenti presentano profili di rischio specifici connessi, tra l'altro, alla rapidità di esecuzione delle operazioni, alla possibile operatività a distanza e all'utilizzo da parte di soggetti diversi dal titolare, che richiedono l'adozione di misure di controllo proporzionate e, ove necessario, rafforzate.

In tale ambito, la Banca:

- assicura che l'emissione e l'utilizzo degli strumenti di pagamento avvengano, di norma, nell'ambito di rapporti continuativi già sottoposti ad adeguata verifica della clientela, in coerenza con il profilo di rischio assegnato;
- applica presidi di identificazione e verifica dell'identità del cliente, anche mediante strumenti di riconoscimento a distanza conformi alla normativa vigente e adeguati livelli di sicurezza;
- definisce limiti operativi e soglie di utilizzo, differenziati in funzione del profilo di rischio della clientela, della tipologia di strumento e delle modalità operative;
- presidia i processi di monitoraggio delle operazioni (*transaction monitoring*), anche attraverso l'utilizzo di strumenti automatizzati, al fine di individuare comportamenti anomali o incoerenti rispetto al profilo economico-finanziario del cliente;
- adotta sistemi di rilevazione e gestione delle frodi, integrati con i presidi antiriciclaggio, al fine di intercettare tempestivamente fenomeni potenzialmente riconducibili a riciclaggio o finanziamento del terrorismo;
- assicura la tracciabilità delle operazioni e la corretta conservazione dei dati e delle informazioni, garantendone completezza, integrità e disponibilità ai fini degli adempimenti normativi;
- garantisce il corretto funzionamento dei flussi di segnalazione interna, assicurando la tempestiva escalation delle operazioni anomale ai fini della valutazione e dell'eventuale inoltro di segnalazioni di operazioni sospette.

Qualora la Banca si avvalga di soggetti terzi per l'emissione o la gestione degli strumenti di pagamento, gli accordi contrattuali disciplinano in modo puntuale le rispettive responsabilità in materia di adempimenti antiriciclaggio, prevedendo adeguati presidi di controllo e flussi informativi verso la Banca.

6 AUTOVALUTAZIONE DEI RISCHI DI RICICLAGGIO E FINANZIAMENTO DEL TERRORISMO

In conformità a quanto stabilito dall'art. 15 del Decreto Antiriciclaggio (D.Lgs. 21 novembre 2007, n. 231), la Banca effettua con cadenza annuale un articolato esercizio di autovalutazione del rischio di riciclaggio e di finanziamento del terrorismo. Tale attività rappresenta uno dei principali strumenti di governance del rischio AML/CTF e consente all'intermediario di analizzare in modo sistematico la propria esposizione ai fenomeni illeciti, verificare l'adeguatezza dei presidi interni e programmare interventi correttivi mirati. L'autovalutazione non si limita a un mero adempimento formale, ma costituisce un processo strutturato, fondato su metodologie definite, che permette di ottenere una visione complessiva, aggiornata e coerente dell'assetto di controllo interno.

L'esercizio si articola nelle seguenti fasi principali, tra loro logicamente interconnesse:

- **Individuazione delle linee di business:** in questa fase preliminare la Banca procede a identificare e mappare le diverse aree operative, i prodotti, i servizi e i canali distributivi attraverso i quali svolge la propria attività. La corretta delimitazione del perimetro operativo è fondamentale per comprendere la natura e la varietà delle esposizioni potenziali al rischio di riciclaggio e finanziamento del terrorismo.

- **Calcolo del rischio inerente:** la Banca analizza le caratteristiche dell'operatività, individuando i fattori di rischio che possono favorire comportamenti illeciti. Tale analisi considera, tra l'altro, la tipologia della clientela, l'area geografica di riferimento, il livello di complessità dei prodotti, il grado di esposizione verso Paesi o operatori a rischio elevato e la frequenza delle operazioni. Il rischio inerente rappresenta quindi la misura del rischio "lordo", prescindendo dai controlli esistenti.
- **Valutazione della vulnerabilità:** a seguito della quantificazione del rischio inerente, la Banca procede alla valutazione della vulnerabilità del proprio sistema di controlli, verificando se i presidi organizzativi, procedurali e tecnologici in essere siano adeguati a mitigare i rischi identificati. Tale giudizio tiene conto della qualità dei processi di adeguata verifica, dei sistemi di monitoraggio, dell'efficacia dei controlli di primo e secondo livello, nonché dell'adeguatezza dei flussi informativi.
- **Determinazione del rischio residuo:** il rischio residuo è il risultato della combinazione tra il livello di rischio inerente e il grado di vulnerabilità. Esso rappresenta la misura del rischio effettivo che permane dopo l'applicazione dei controlli e consente di individuare eventuali aree operative o processi che richiedono interventi di rafforzamento.
- **Identificazione delle azioni di rimedio:** sulla base delle aree di rischio che emergono dall'analisi, la Banca definisce un piano di interventi correttivi volti a colmare le eventuali lacune riscontrate. Gli interventi possono riguardare l'aggiornamento delle procedure, il potenziamento dei sistemi informatici, l'introduzione di nuovi controlli, la revisione dei processi di onboarding, la formazione del personale o la ridefinizione delle responsabilità operative. L'obiettivo è garantire un miglioramento continuo della capacità preventiva dell'ente.

Al termine del processo, gli esiti dell'autovalutazione vengono riportati nella Relazione annuale predisposta dalla Funzione Antiriciclaggio, la quale li sottopone agli Organi Societari competenti per la relativa approvazione. Successivamente, la documentazione viene trasmessa alla competente Autorità di Vigilanza, quale dimostrazione del livello di presidio del rischio AML/CTF della Banca e della coerenza del sistema di controllo interno con gli obblighi normativi vigenti.

Per la descrizione precisa del processo di Autovalutazione si invia al documento "Metodologia per l'autovalutazione dei rischi di riciclaggio e di finanziamento del terrorismo" di Banca Cambiano.

7 FORMAZIONE

La Banca adotta programmi di formazione e aggiornamento professionale permanenti, finalizzati alla corretta applicazione delle disposizioni previste nel Decreto Antiriciclaggio, al riconoscimento di operazioni connesse al riciclaggio e al finanziamento del terrorismo e all'adozione dei comportamenti e delle procedure da utilizzare. Particolare attenzione formativa è rivolta al personale che ha un contatto diretto con la clientela ed al personale di nuova assunzione.

L'attività di qualificazione e aggiornamento professionale riveste carattere di continuità e di sistematicità nell'ambito dei programmi organici che tengono conto dell'evoluzione della normativa (interna ed esterna) e delle procedure.

L'addestramento e la formazione assicurano una specifica preparazione del personale a più diretto contatto con la clientela o comunque coinvolto nel processo di segnalazione di operazioni sospette nonché di quello addetto alla funzione antiriciclaggio. In particolare, la formazione viene strutturata per livelli, in funzione della rilevanza e delle responsabilità assegnate alle diverse funzioni aziendali.

L'attività di formazione in materia antiriciclaggio e antiterrorismo viene svolta dalla Banca con periodicità almeno annuale, avvalendosi di personale interno e/o di specialisti terzi. Nel caso di ricorso a fornitori esterni il Responsabile AML accerta che i soggetti cui sia affidato lo svolgimento dell'attività formativa possiedano le conoscenze in materia di antiriciclaggio richieste per garantire la qualità della formazione e che il contenuto di questa sia adeguato alle specificità del destinatario. I programmi di formazione adottati garantiscono un adeguato aggiornamento professionale di tutte le funzioni aziendali.

I soggetti partecipanti alle attività formative antiriciclaggio devono compilare e siglare l'apposito registro di presenza al fine di certificare l'avvenuta partecipazione degli stessi e sostenere un test di valutazione finale sulle competenze acquisite.

Inoltre, è previsto un apposito programma formativo in materia di antiriciclaggio rivolto agli Organi Aziendali (Consiglio di Amministrazione) e al management della Banca (Direttore Generale e Responsabili di Funzione) con la finalità di fornire a tali soggetti una visione d'insieme del quadro normativo in materia, analizzare le regole di riferimento e il ruolo delle strutture aziendali.

La Banca promuove l'informazione e comunicazione dei presidi adottati a tutta la struttura aziendale, al fine di ottemperare a quanto previsto dal vigente dettato normativo che all'art. 16, comma 3 del Decreto stabilisce che, "i soggetti obbligati garantiscono lo svolgimento di programmi permanenti di formazione, finalizzati alla corretta applicazione delle disposizioni di cui al presente decreto, al riconoscimento di operazioni connesse al riciclaggio o al finanziamento del terrorismo e all'adozione dei comportamenti e delle procedure da adottare".

A tal fine, la presente policy, il regolamento in materia di antiriciclaggio e il materiale utilizzato per la formazione è messo a disposizione del personale della Banca nelle cartelle di rete ovvero nei sistemi informativi aziendali.

8 SANZIONI

Ai sensi del D.Lgs. 21 novembre 2007, n. 231, la violazione degli obblighi previsti in materia di contrasto del riciclaggio e del finanziamento del terrorismo comporta l'applicazione di sanzioni amministrative e penali, differenziate in funzione della gravità e della tipologia dell'adempimento omesso o irregolarmente svolto.

In particolare:

- Violazioni degli obblighi di adeguata verifica della clientela; l'omissione totale o parziale degli obblighi di identificazione del cliente, del titolare effettivo o di acquisizione delle informazioni sullo scopo e sulla natura del rapporto, può comportare l'applicazione di sanzioni amministrative pecuniarie rilevanti, proporzionate al fatturato e alla gravità dell'infrazione, come previsto dagli artt. 55 e 56 del Decreto.
- Violazioni degli obblighi di registrazione e conservazione dei dati; l'inosservanza degli obblighi di corretta conservazione della documentazione e dei dati rilevanti ai fini antiriciclaggio determina l'applicazione di sanzioni amministrative che possono essere elevate, con valori massimi incrementati nei casi di violazioni gravi, ripetute o sistematiche, conformemente all'art. 57 del Decreto.
- Violazioni degli obblighi di segnalazione delle operazioni sospette (SOS); la mancata segnalazione di operazioni sospette all'Unità di Informazione Finanziaria (UIF), quando dovuta, espone l'ente e i soggetti responsabili a sanzioni amministrative pecuniarie significative e, nei casi più rilevanti o connotati da dolo, può integrarsi in responsabilità penale ai sensi dell'art. 55 del Decreto.
- Violazioni delle misure restrittive dell'Unione Europea; la violazione degli obblighi imposti dalle misure restrittive in termini di congelamento dei fondi, restrizioni commerciali, finanziarie e settoriali e/o degli obblighi informativi verso la UIF e/o il Comitato di sicurezza Finanziaria determina l'applicazione di sanzioni amministrative, nonché misure interdittive.
- Ostacolo alle attività di vigilanza; il rifiuto, l'omissione o l'invio di informazioni incomplete o non veritiere alle autorità competenti costituisce violazione sanzionabile con sanzioni amministrative anche di natura interdittiva, previste dall'art. 62, che possono includere limitazioni temporanee all'operatività.
- Responsabilità dell'ente: le violazioni sistematiche o particolarmente gravi possono esporre la Società a misure correttive, sanzioni amministrative aggiuntive e potenziali impatti reputazionali. I responsabili interni sono tenuti a collaborare pienamente con le Autorità e ad adottare tempestivamente misure correttive.

L'identificazione puntuale delle sanzioni applicabili e le modalità di informazione, formazione e messa a conoscenza del personale della Banca in merito agli obblighi antiriciclaggio e ai relativi profili sanzionatori sono disciplinate nel Regolamento interno in materia di prevenzione del riciclaggio e del finanziamento del terrorismo, che recepisce e dettaglia quanto previsto dal D.Lgs. 21 novembre 2007, n. 231, e costituisce parte integrante del presente impianto normativo aziendale.