

LINEE GUIDA PER IL CONTRASTO AI FENOMENI DI RICICLAGGIO, DI FINANZIAMENTO DEL TERRORISMO E PER LA GESTIONE DEGLI EMBARGHI

Normativa attinente ad aree sensibili relative al D. Lgs. 231/01

Area di rischio: Reati contro la Pubblica Amministrazione

Protocolli: Gestione dei rapporti con le Autorità di Vigilanza

Area di rischio: Reati con finalità di terrorismo o di eversione dell'ordine democratico, i reati di criminalità organizzata, i reati transnazionali, i reati contro la persona ed i reati in materia di frodi sportive e di esercizio abusivo di gioco o di scommessa

Area di rischio: Reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché autoriciclaggio

Protocolli: Contrasto finanziario al terrorismo ed al riciclaggio dei proventi di attività criminose

Area di rischio: Reati informatici

Protocolli: Gestione e utilizzo dei sistemi informatici e del Patrimonio Informativo di Gruppo

Area di rischio: Reati tributari

Protocolli: Gestione dei rischi e degli adempimenti ai fini della prevenzione dei reati tributari

Struttura Responsabile del documento:
Direzione Centrale Anti Financial Crime

Destinatari:
Gruppo Intesa Sanpaolo

Percorso:
ARCO – Documenti di Governance – Linee Guida – Gestione Rischi e Controlli

Decorrenza: aprile 2022

INDICE

PREMESSA	4
1. IL CONTESTO NORMATIVO	6
1.1 Il contesto normativo in materia di antiriciclaggio e di contrasto al finanziamento del terrorismo.....	6
1.2 Il contesto normativo in materia di embarghi	8
2. PRINCIPI GENERALI DEL MODELLO DI GOVERNO	11
3. RUOLI E RESPONSABILITÀ	12
3.1 Organi Societari.....	12
3.2 Organismo di Vigilanza ai sensi del D. Lgs. n. 231/2001	12
3.3 Area di Governo Chief Compliance Officer	12
3.3.1 Direzione Centrale Anti Financial Crime	12
3.3.1.1 Responsabile della Funzione Antiriciclaggio.....	16
3.3.1.2 Responsabile delle segnalazioni di operazioni sospette.....	17
3.3.1.3 Referente S.AR.A. (Segnalazioni AntiRiciclaggio Aggregate)	18
3.3.1.4 Tavolo di gestione e supervisione degli scenari	18
3.3.2 Direzione Centrale Compliance Governance e Controlli.....	19
3.3.3 Compliance Digital Transformation.....	19
3.4 Area di Governo Chief Risk Officer	19
3.5 Chief Audit Officer.....	20
3.6 Area di Governo Chief Operating Officer	21
3.6.1 Direzione Centrale Organizzazione	21
3.6.2 Direzione Centrale Politiche di Sviluppo e Learning Academy	21
3.6.3 Direzione Centrale People Management & HR Transformation	22
3.6.4 Direzione Centrale Affari Sindacali e Politiche del Lavoro	22
3.7 Area di Governo Chief IT, Digital and Innovation Officer	22
3.7.1 Transformation Center	22
3.7.2 Direzione Centrale Operations.....	23
3.7.3 Digital Business Partner	23
3.7.4 Direzione Centrale Sistemi Informativi	24
3.7.5 Direzione Centrale Cybersecurity and Business Continuity Management ...	24
3.7.6 Direzione Centrale Data Office	24
3.8 Area di Governo Chief Governance Officer	25
3.8.1 Direzione Centrale Legale e Contenzioso – Group General Counsel.....	25
3.9 Area di Governo Chief Institutional Affairs and External Communication Officer	25
3.9.1 Direzione Centrale Institutional Affairs e struttura International Public Affairs	25
3.10 Divisioni	25
3.11 Altre funzioni organizzative	27
4. MACRO-PROCESSI PER IL CONTRASTO AI FENOMENI DI RICICLAGGIO, DI FINANZIAMENTO DEL TERRORISMO E PER LA GESTIONE DEGLI EMBARGHI	28
4.1 Definizione delle linee guida e delle regole metodologiche	28
4.2 AFC Risk Assessment e Risk Appetite Framework	28
4.3 Programmazione delle attività	30
4.4 Allineamento normativo	30
4.5 Consulenza e clearing	31
4.6 Assurance.....	31
4.6.1 Il modello di assurance	31

4.6.2	Metodologia di svolgimento delle attività	32
4.6.3	Interazioni con le altre funzioni di controllo e flussi informativi.....	33
4.6.4	Processo di follow up.....	33
4.7	Diffusione della cultura in materia di antiriciclaggio, contrasto al finanziamento del terrorismo ed embarghi	34
4.8	Interazione con le Autorità di Vigilanza e gestione degli eventi di non conformità.....	34
4.9	Adempimenti specifici	35
4.9.1	Adeguata verifica della clientela	35
4.9.1.1	Obblighi ordinari di adeguata verifica.....	36
4.9.1.2	Operatività a distanza	37
4.9.1.3	Obblighi semplificati di adeguata verifica.....	37
4.9.1.4	Obblighi rafforzati di adeguata verifica.....	38
4.9.1.5	Esecuzione degli obblighi di adeguata verifica da parte di terzi.....	39
4.9.2	Conservazione e messa a disposizione dei documenti, dei dati e delle informazioni	40
4.9.3	Monitoraggio delle transazioni	40
4.9.3.1	Monitoraggio dei trasferimenti di fondi.....	41
4.9.4	Segnalazione delle Operazioni Sospette.....	41
4.9.5	Gestione del rischio in ambito extra SEE.....	42
4.10	Flussi informativi agli Organi Societari.....	42
5.	INDIRIZZO E COORDINAMENTO DEL GRUPPO	43
5.1	Il modello di gestione accentrata	44
5.2	Il modello di indirizzo, coordinamento e controllo	45

PREMESSA

Il Gruppo Intesa Sanpaolo riconosce il rilievo strategico del presidio del rischio di non conformità e del rischio di condotta, nel cui ambito si colloca il sistema di governo per il contrasto ai fenomeni di riciclaggio (c.d. “Anti-Money Laundering” o “AML”), di finanziamento del terrorismo (c.d. “Counter Financing Terrorism” o “CFT”) e per la gestione degli embarghi (c.d. “Financial Sanctions”).

Le Linee Guida oggetto del presente documento, redatte anche in ottemperanza ai Provvedimenti della Banca d’Italia del 26 marzo e del 30 luglio 2019¹, individuano i principi di riferimento e definiscono il modello di gestione dei rischi in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi del Gruppo Intesa Sanpaolo, delineando:

- i principi generali del modello di governo;
- i ruoli e le responsabilità degli Organi e delle strutture aziendali coinvolte;
- i macro-processi per il contrasto ai fenomeni di riciclaggio, di finanziamento del terrorismo e per la gestione degli embarghi;
- le modalità di governo delle Banche/Società del Gruppo e delle Filiali Estere.

Le Linee Guida sono oggetto di riesame su base annuale e le eventuali modifiche sono sottoposte all’approvazione del Consiglio di Amministrazione, previo esame del Comitato Rischi e del Comitato per il Controllo sulla Gestione.

Le Linee Guida trovano la loro declinazione operativa nelle Regole per la Gestione dei Macro-Processi di Compliance (“Compliance Rulebook”) e nelle Regole aziendali in ambito di antiriciclaggio, contrasto al finanziamento del terrorismo e gestione degli embarghi, volte a definire i singoli adempimenti specifici. Il Compliance Rulebook è oggetto di riesame almeno su base annuale, in coerenza con l’evoluzione organizzativa ed operativa del modello di presidio dei rischi di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi e le eventuali modifiche sono approvate dal Chief Compliance Officer e sottoposte all’attenzione del Comitato per il Controllo sulla Gestione. Il Compliance Rulebook è emanato con Nota Interna del Chief Compliance Officer.

Per “riciclaggio” si intende:

- 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. Costituisce riciclaggio anche l’uso e l’occultamento dei proventi criminali da parte delle persone che hanno commesso il reato che ha generato tali proventi (cosiddetto “autoriciclaggio”);
- 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;
- 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;
- la partecipazione ad uno degli atti di cui ai punti 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 agevolarne l’esecuzione.

Per “finanziamento del terrorismo” si intende qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all’intermediazione, al deposito, alla custodia o all’erogazione, in qualunque modo realizzate, di fondi e risorse economiche, direttamente o indirettamente, in tutto o in parte, utilizzabili per il compimento di una o più condotte, con finalità di terrorismo secondo quanto

¹ Tali Provvedimenti prevedono, infatti, inter alia l’approvazione da parte dell’organo con funzione di supervisione strategica di apposita “policy antiriciclaggio”.

previsto dalle leggi penali, ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette.

Si definisce “embargo” il divieto di commercio e di scambio con Paesi sanzionati, al fine di isolare e mettere i loro governi in una difficile situazione politica ed economica interna.

1. IL CONTESTO NORMATIVO

1.1 *Il contesto normativo in materia di antiriciclaggio e di contrasto al finanziamento del terrorismo*

La principale normativa di riferimento per la prevenzione ed il contrasto del riciclaggio di denaro e del finanziamento del terrorismo può essere suddivisa nelle seguenti categorie:

- normativa dell'Unione Europea;
- normativa primaria e secondaria italiana.

La principale normativa dell'Unione Europea è contenuta nelle seguenti fonti:

- Direttiva (UE) 2015/849 del Parlamento Europeo e del Consiglio del 20/05/2015 (la "IV Direttiva") relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, che modifica il Regolamento (UE) n. 648/2012 del Parlamento Europeo e del Consiglio e che abroga la Direttiva 2005/60/CE del Parlamento Europeo e del Consiglio e la Direttiva 2006/70/CE della Commissione;
 - Direttiva (UE) 2018/843 del Parlamento Europeo e del Consiglio del 30/05/2018 (la "V Direttiva") che modifica la Direttiva (UE) 2015/849;
 - Direttiva (UE) 2018/1673 del Parlamento Europeo e del Consiglio del 23/10/2018 sulla lotta al riciclaggio mediante il diritto penale;
 - Regolamento (UE) 2015/847 del Parlamento Europeo e del Consiglio del 20/05/2015 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il Regolamento (CE) n. 2006/1781;
 - Regolamento Delegato (UE) 2016/1675, e successive modifiche, che integra la IV Direttiva individuando i Paesi terzi ad alto rischio con carenze strategiche;
 - Regolamento Delegato (UE) 2019/758 della Commissione che integra la IV Direttiva definendo l'azione minima e il tipo di misure supplementari che gli enti creditizi e gli istituti finanziari con succursali o filiazioni in Paesi terzi al di fuori dello Spazio Economico Europeo ("Paesi extra SEE") devono intraprendere per mitigare il rischio di riciclaggio e di finanziamento del terrorismo;
- e, specificamente in materia di contrasto al finanziamento del terrorismo:
- Regolamento 2580/2001/CE del Consiglio del 27/12/2001 relativo a misure restrittive specifiche, contro determinate persone ed entità, destinate a combattere il terrorismo;
 - Regolamento 881/2002/CE del Consiglio del 27/05/2002 che impone specifiche misure restrittive nei confronti di determinate persone ed entità (elencate nell'allegato al Regolamento medesimo) associate a Osama bin Laden, alla rete Al-Qaeda e ai Talebani.

La principale normativa primaria italiana è contenuta nelle seguenti fonti legislative:

- D. Lgs. n. 231/2007, come modificato dal D. Lgs. n. 125/2019 che ha aggiornato il quadro normativo italiano antiriciclaggio recependo la V Direttiva, e da ultimo dalla L. n. 120/2020 e dalla L. n. 15/2022;
- D. Lgs. n. 109/2007, come modificato dal D. Lgs. n. 90/2017, recante misure per prevenire, contrastare e reprimere il finanziamento del terrorismo internazionale, che impone obblighi di comunicazione di beni e risorse congelate e di segnalazione di operazioni sospette;
- D. Lgs. n. 195/2021 che ha dato attuazione alla Direttiva (UE) 2018/1673.

La principale normativa secondaria, emanata dalla Banca d'Italia e dall'Unità di Informazione Finanziaria ("UIF"), è contenuta nelle seguenti fonti regolamentari:

- Provvedimento del 24 agosto 2010 recante gli indicatori di anomalie per gli intermediari al fine di agevolare l'individuazione di operazioni sospette;
- Provvedimento del 26 marzo 2019 recante disposizioni attuative in materia di organizzazione, procedure e controlli interni volti a prevenire l'utilizzo degli intermediari e degli altri soggetti che svolgono attività finanziaria ai fini di riciclaggio e di finanziamento del terrorismo;
- Provvedimento del 28 marzo 2019 recante istruzioni in materia di comunicazioni oggettive;

- Provvedimento del 30 luglio 2019 recante disposizioni attuative in materia di adeguata verifica della clientela;
- Provvedimento del 24 marzo 2020 recante disposizioni attuative per la conservazione e messa a disposizione dei documenti, dei dati e delle informazioni per il contrasto del riciclaggio e del finanziamento del terrorismo;
- Provvedimento del 25 agosto 2020 recante disposizioni per l'invio delle segnalazioni antiriciclaggio aggregate;
- Orientamenti dell'Autorità bancaria europea in materia di fattori di rischio per l'adeguata verifica della clientela (EBA/GL/2021/02), attuati con Nota n. 15 del 4 ottobre 2021.

Assume inoltre particolare rilevanza, stante l'operatività del Gruppo Intesa Sanpaolo negli Stati Uniti, la normativa emanata dalle Autorità statunitensi contenuta principalmente nelle seguenti fonti:

- Bank Secrecy Act – BSA (1970), disegnato per identificare la fonte, il volume e la valuta di strumenti finanziari che fluiscono da o verso gli Stati Uniti o depositati nelle istituzioni finanziarie statunitensi;
- US Patriot Act (Uniting and Strengthening America by Providing Appropriate Tool to Intercept and Obstruct Terrorism - 2001) che, emanato a seguito degli attacchi terroristici dell'11 settembre 2001, estende i requisiti del BSA, richiede alle istituzioni finanziarie la predisposizione di procedure di due diligence e migliora la condivisione delle informazioni tra le istituzioni finanziarie e il Governo USA;
- Law 302 - Section 504 (NYSDFS Rule on Transaction Monitoring and Filtering - 2017) che stabilisce uno standard minimo per il monitoraggio delle transazioni e le sanzioni per le banche soggette alla legge di New York, sotto la giurisdizione del New York State Department of Financial Services;
- Department of the Treasury Financial Crimes Enforcement Network, '31 Code of Federal Regulation Parts 1010, 1020, 1023, 1024 and 1026 Customer Due Diligence Requirements for Financial Institutions' che definisce i nuovi requisiti in tema di identificazione del titolare effettivo delle Financial Institutions e stabilisce un approccio al controllo basato su criteri sia sostanziali sia formali;
- Anti-Money Laundering Act of 2020, divenuto legge nel gennaio 2021, che prevede tra le numerose disposizioni (i) l'istituzione di un database di registrazione della titolarità effettiva che sarà implementato dal Financial Crimes Enforcement Network (FinCEN) e (ii) il nuovo Bank Secrecy Act con sanzioni rafforzate per i trasgressori recidivi e gravi.

In quanto presente negli Stati Uniti, Intesa Sanpaolo ha sottoscritto il documento "US Patriot Act Certification" ed è tenuta ad assoggettare anche alla normativa statunitense l'operatività commerciale e finanziaria nel territorio statunitense, quale l'esecuzione degli ordini di pagamento in dollari e, in generale, l'attività di natura transazionale svolta sia per proprio conto che per conto di terzi. Sono inoltre assoggettate alla normativa statunitense le operazioni che la Banca effettua per proprio conto e/o per conto dei propri clienti quando tali operazioni comportino una relazione con nominativi soggetti alla normativa americana (ad esempio, banche USA, filiali estere di banche USA e comunque, in generale, US Subject).

I principi comuni del contesto normativo di riferimento sono:

- l'obbligo di effettuare l'adeguata verifica della clientela, acquisendo le informazioni idonee ad identificare il cliente, il titolare effettivo e lo scopo del rapporto o dell'operazione;
- l'obbligo di conservazione dei dati, delle informazioni e dei documenti per gli adempimenti antiriciclaggio;
- l'obbligo di monitorare costantemente l'operatività del rapporto instaurato;
- l'obbligo di segnalazione delle operazioni sospette nell'ottica di una fattiva collaborazione con le Autorità;
- l'obbligo di astensione dall'apertura di un nuovo rapporto, dall'esecuzione di un'operazione occasionale o dal mantenimento di un rapporto in essere nel caso non sia possibile completare l'adeguata verifica ovvero sussista il sospetto di riciclaggio di denaro o di finanziamento del terrorismo;

- l'obbligo dell'Organo con funzione di controllo di comunicare le eventuali infrazioni rilevanti di cui venga a conoscenza nell'esercizio dei propri compiti;
- l'obbligo della formazione adeguata del personale per garantire la corretta applicazione delle disposizioni.

Per il rispetto di tali obblighi i soggetti destinatari devono individuare funzioni organizzative, risorse e procedure coerenti e proporzionate alla tipologia dell'attività svolta, alle loro dimensioni, complessità organizzativa e caratteristiche operative.

L'organizzazione richiesta dalla normativa deve essere contraddistinta da:

- l'istituzione di un'apposita funzione deputata a prevenire e contrastare la realizzazione di operazioni di riciclaggio e di finanziamento del terrorismo, la nomina del suo responsabile e del responsabile delegato per la segnalazione delle operazioni sospette di riciclaggio e di finanziamento del terrorismo;
- una chiara definizione di ruoli, compiti e responsabilità nonché procedure che garantiscano l'osservanza degli obblighi di adeguata verifica della clientela, di conservazione della documentazione e delle evidenze dei rapporti e delle operazioni e di segnalazione delle operazioni sospette;
- un'architettura delle funzioni di controllo coordinata nelle sue componenti, anche mediante idonei flussi informativi, e adeguata alla dimensione aziendale e alla sua complessità, alla tipologia dei servizi e prodotti offerti nonché all'entità del rischio associabile alle caratteristiche della clientela;
- una forte responsabilizzazione del personale dipendente e dei collaboratori esterni e un'attività di controllo idonea a monitorare il rispetto, da parte dei medesimi, degli obblighi normativi e dei processi interni nonché della loro attuazione.

La normativa richiede un efficace coordinamento dei presidi per la prevenzione ed il contrasto del riciclaggio di denaro e del finanziamento del terrorismo a livello di Gruppo e che le procedure in essere presso le Società e le Filiali Estere siano in linea con gli standard del Gruppo e tali da assicurare la condivisione delle informazioni a livello consolidato. In presenza di Paesi extra SEE che pongono limiti alla circolazione delle informazioni vanno adottate specifiche misure correttive in coerenza con le previsioni del richiamato Regolamento Delegato (UE) 2019/758.

1.2 Il contesto normativo in materia di embarghi

La Carta delle Nazioni Unite conferisce al Consiglio di Sicurezza dell'ONU il potere di decidere, in maniera vincolante per tutti i membri delle Nazioni Unite, misure restrittive finalizzate a favorire il mantenimento o il ripristino della pace e della sicurezza internazionale. Il Trattato sull'Unione Europea e il Trattato sul funzionamento dell'Unione Europea prevedono che gli Stati Membri assumano una posizione comune nell'interrompere o limitare le relazioni economiche e finanziarie con uno o più Paesi terzi. Le suddette misure hanno lo scopo di:

- salvaguardare i valori comuni, gli interessi fondamentali, la sicurezza, l'indipendenza e l'integrità dell'Unione Europea;
- consolidare e sostenere la democrazia, lo Stato di diritto, i diritti dell'uomo e i principi del diritto internazionale;
- preservare la pace e rafforzare la sicurezza internazionale, in conformità agli obiettivi e ai principi della Carta delle Nazioni Unite;
- promuovere la cooperazione internazionale.

Esistono altresì fonti di normativa internazionale che istituiscono un particolare regime di divieto o prevedono delle limitazioni a investire in determinati settori industriali o a importare/esportare da e verso i Paesi "a rischio elevato o significativo".

La normativa di riferimento per la gestione degli embarghi può quindi essere suddivisa nelle seguenti categorie:

- normativa emanata dall'ONU;
- normativa europea;
- normativa primaria e secondaria italiana.

La principale normativa emanata dall'ONU è contenuta nelle seguenti fonti:

- Risoluzioni adottate dal Consiglio di Sicurezza ai sensi dell'art. 41 del Capitolo VII della Carta delle Nazioni Unite con cui vengono imposte le misure restrittive relative a soggetti e/o Paesi.

La principale normativa europea è contenuta nella seguente fonte:

- Regolamento (UE) 2021/821 del Parlamento europeo e del Consiglio del 20 maggio 2021 che istituisce un regime dell'Unione di controllo delle esportazioni, dell'assistenza tecnica, dell'intermediazione, del transito e del trasferimento dei prodotti a duplice uso.

La normativa primaria italiana è contenuta nelle seguenti fonti legislative:

- Legge n. 185/1990 e successive modifiche recante "Nuove norme sul controllo dell'esportazione, importazione e transito dei materiali di armamento" che costituisce tuttora la base della disciplina in materia di trasferimenti di beni classificati "materiali d'armamento";
- D. Lgs. n. 221/2017 che ha riordinato e semplificato la disciplina delle procedure di autorizzazione all'esportazione di prodotti e tecnologie a duplice uso e delle sanzioni in materia di embarghi commerciali, nonché per ogni tipologia di operazione di esportazione di materiali proliferanti. Il decreto legislativo prevede (artt. da 18 a 21) l'applicazione di sanzioni penali e amministrative a carico di chi effettua operazioni di esportazione di beni "dual use" in violazione della normativa.

La principale normativa secondaria è contenuta nella seguente fonte regolamentare emanata dalla Banca d'Italia:

- Provvedimento 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.

Assume inoltre particolare rilevanza, stante l'operatività del Gruppo Intesa Sanpaolo negli Stati Uniti, la normativa emanata dalle Autorità statunitensi, contenuta - oltre che nel "US Patriot Act" già sopra richiamato - nei provvedimenti relativi alle sanzioni economiche e commerciali decise tempo per tempo dal Governo USA, principalmente tramite l'Office of Foreign Assets Control (OFAC) del Dipartimento del Tesoro, nell'ambito di scelte di politica estera e sicurezza nazionale².

Il contesto normativo di riferimento, che presenta evidenti correlazioni con quello già illustrato in tema di contrasto al riciclaggio ed al finanziamento del terrorismo, prevede misure restrittive e sanzionatorie a carico sia di governi di Paesi terzi, sia di entità non statali, persone fisiche o giuridiche in materia di:

- embarghi sulle armi;
- altre restrizioni commerciali specifiche o generali (divieto di esportazione e di importazione);
- restrizioni finanziarie (congelamento di beni e risorse, divieti riguardanti transazioni finanziarie, restrizioni relative ai crediti all'esportazione o agli investimenti compresi quelli in strumenti finanziari);
- sanzioni penali a carico di chi finanzia associazioni terroristiche od eversive e di chi effettua operazioni di esportazione di beni in violazione delle norme in materia di "dual use".

La normativa di riferimento richiede alla Banca la previsione di misure che garantiscano:

- controlli anagrafici e transazionali sulle operazioni effettuate dai propri clienti e correlate a importazioni e/o esportazioni;
- controlli sull'operatività in strumenti finanziari;

² Alla data di pubblicazione delle presenti Linee Guida rientrano in tali ambiti principalmente i provvedimenti emanati nei confronti dell'Iran, della Siria, della Corea del Nord, di Cuba e della regione Crimea.

- la tracciabilità dei controlli effettuati sulle operazioni provenienti da/dirette verso i Paesi, le persone e le entità nei cui confronti sono stabilite restrizioni;
- il congelamento di beni e risorse riconducibili ai soggetti designati, destinatari delle misure restrittive, e l'inoltro delle conseguenti comunicazioni all'UIF;
- la segnalazione di operazioni sospette di finanziamento del terrorismo o di attività di proliferazione di armi di distruzione di massa.

2. PRINCIPI GENERALI DEL MODELLO DI GOVERNO

Le presenti Linee Guida si collocano nell'ambito dell'architettura definita dal Gruppo attraverso il Regolamento del Sistema dei Controlli Interni Integrato ("Regolamento SCII").

Il presidio del rischio in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi è, infatti, parte integrante di tale sistema e viene perseguito attraverso l'operare sinergico di tutte le componenti aziendali, in coerenza con quanto previsto dal Provvedimento della Banca d'Italia del 26 marzo 2019 in materia di organizzazione, procedure e controlli interni³. In particolare:

- gli Organi Societari assicurano, ciascuno secondo le proprie competenze e responsabilità, l'adeguato presidio dei rischi in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi;
- l'Organismo di Vigilanza ai sensi del D. Lgs. n. 231/2001 vigila sull'efficace attuazione, sul funzionamento, sull'osservanza e sull'aggiornamento del relativo Modello e sulla sua adeguatezza a prevenire e contrastare la commissione dei reati presupposto di tale Decreto;
- la Funzione Antiriciclaggio verifica nel continuo l'efficacia dei processi e delle procedure aziendali e propone, in collaborazione con le competenti funzioni aziendali, le modifiche organizzative e procedurali necessarie e/o opportune per assicurare un adeguato presidio del rischio di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi;
- le altre funzioni aziendali di controllo di secondo livello e le funzioni di supporto collaborano con la Funzione Antiriciclaggio affinché quest'ultima sviluppi le proprie metodologie di gestione del rischio in modo coerente con le strategie e l'operatività aziendale;
- le funzioni operative, di business e di supporto si attengono ai processi ed alle procedure aziendali, verificandone l'applicazione con adeguati controlli di primo livello in un'ottica di piena e completa aderenza alle norme e agli standard applicabili;
- la Funzione di internal audit, nell'ambito della propria attività verifica in modo continuativo il grado di adeguatezza dell'assetto organizzativo aziendale nonché la sua conformità rispetto alla disciplina di riferimento e vigila sulla funzionalità del complessivo sistema dei controlli interni.

Nel presidio dei rischi in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi, il Gruppo Intesa Sanpaolo adotta i seguenti principi generali:

- ispirazione a valori di onestà, correttezza e responsabilità; ciò nel rispetto sostanziale del Codice Etico di Gruppo;
- collaborazione attiva con le Autorità di Vigilanza nella prevenzione dei fenomeni in questione, tenuto conto delle prescrizioni normative in materia di riservatezza delle segnalazioni e delle informazioni relative alle operazioni sospette e di protezione dei dati personali (privacy) e del segreto bancario;
- adozione di standard di presidio in termini di linee guida, regole, metodologie, processi e strumenti allineati agli standard internazionali in materia e ragionevolmente omogenei a livello di Gruppo, nel rispetto delle normative applicabili a livello locale;
- adozione di misure di presidio "risk based" proporzionate a caratteristiche e complessità dell'attività svolta e alla forma giuridica, alle dimensioni e all'articolazione organizzativa delle diverse entità del Gruppo.

Il modello di governo vede il progressivo ricorso a Competence Center specializzati nel monitoraggio delle transazioni (Competence Center di Transaction Monitoring) e nell'adeguata verifica della clientela (Competence Center di Know Your Customer).

³ La valutazione dei rischi di riciclaggio e di finanziamento del terrorismo è recepita anche nell'ambito del processo di revisione e valutazione prudenziale (c.d. SREP); cfr. pubblicazione in data 18/3/2022 da parte di EBA dell'aggiornamento alle "Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing"

3. RUOLI E RESPONSABILITÀ

3.1 *Organi Societari*

Gli Organi Societari della Capogruppo sono responsabili, ciascuno secondo le proprie competenze e prerogative, di assicurare l'adeguato presidio dei rischi in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi ai quali il Gruppo è o potrebbe essere esposto. L'articolazione dei compiti e delle responsabilità attribuiti agli Organi Societari della Capogruppo è declinata nei relativi Regolamenti e, con riferimento al sistema dei controlli interni, nel "Regolamento SCII".

3.2 *Organismo di Vigilanza ai sensi del D. Lgs. n. 231/2001*

I compiti e i poteri dell'Organismo di Vigilanza sono descritti nel Modello di Organizzazione, gestione e controllo ai sensi del D. Lgs. n. 231/2001. L'Organismo di Vigilanza ha, in particolare, il compito di vigilare continuamente sull'efficace attuazione, sul funzionamento, sull'osservanza e sull'aggiornamento di tale Modello e sulla sua adeguatezza a prevenire e contrastare la commissione dei reati presupposto indicati da tale Decreto, tra cui rientra la normativa antiriciclaggio e di contrasto al finanziamento del terrorismo.

3.3 *Area di Governo Chief Compliance Officer*

I compiti e le responsabilità dell'Area di Governo Chief Compliance Officer e delle strutture a suo diretto riporto sono descritti nei "Funzionigrammi delle strutture", nel "Regolamento SCII" e nelle Linee Guida di Compliance di Gruppo.

Il Chief Compliance Officer assicura il presidio dei rischi in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi tramite la Direzione Centrale Anti Financial Crime, alla quale compete il ruolo di "Funzione Antiriciclaggio di Capogruppo", e tramite la Direzione Centrale Compliance Governance e Controlli e la Compliance Digital Transformation.

3.3.1 *Direzione Centrale Anti Financial Crime*

I compiti e le responsabilità della Direzione Centrale Anti Financial Crime sono descritti nel "Funzionigramma della struttura" e nel "Regolamento SCII".

La Direzione Centrale Anti Financial Crime, in qualità di Funzione Antiriciclaggio:

- è indipendente dalle strutture operative in ragione della sua dipendenza dall'Area di Governo Chief Compliance Officer ed è dotata di risorse qualitativamente e quantitativamente adeguate ai propri compiti;
- riferisce direttamente agli Organi di Vertice;
- ha accesso a tutte le attività dell'impresa nonché a qualsiasi informazione rilevante per lo svolgimento dei propri compiti.

La Direzione Centrale Anti Financial Crime presidia i rischi in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi svolgendo le seguenti attività:

- definisce le linee guida, le regole metodologiche ed i processi da adottare per la gestione del rischio;
- presidia il processo di AFC Risk Assessment, attraverso la predisposizione e la gestione degli strumenti a supporto e delle base dati, nonché la sua integrazione nel Risk Appetite Framework ("RAF"), e procede alla programmazione degli interventi di gestione;
- presidia il processo di allineamento normativo, garantendo che la normativa esterna sia costantemente monitorata ed adeguatamente tradotta in linee guida, regole, processi e procedure interne;

- presta consulenza ed assistenza agli Organi societari ed alle altre strutture della Banca sull'interpretazione e sull'applicazione della normativa esterna ed interna;
- valuta preventivamente, sia su richiesta specifica sia attraverso i processi interni di Product Governance e di clearing, la conformità alla regolamentazione applicabile dei progetti innovativi, ivi inclusi l'avvio di nuove attività e l'inserimento in nuovi mercati, di nuovi prodotti e servizi da avviare alla commercializzazione e di fattispecie ed operazioni sensibili, ivi comprese le Operazioni di Maggior Rilievo;
- fissa gli obiettivi di controllo per mitigare il rischio, coopera con le altre strutture aziendali nella definizione dei controlli di primo e secondo livello e ne esamina le risultanze per la definizione ed il monitoraggio degli interventi di mitigazione;
- presidia le attività di quality assurance e svolge controlli di secondo livello di testing sugli adempimenti stabiliti dalla normativa mirati a valutare (i) la corretta applicazione del processo, o delle sue singole fasi e (ii) la coerenza delle determinazioni assunte nel processo;
- collabora per la diffusione, a tutti i livelli aziendali, di un'adeguata cultura del rischio;
- provvede a gestire le relazioni con le Autorità di Vigilanza e gli eventi di non conformità;
- predispone le relazioni periodiche agli Organi Societari;
- presidia gli adempimenti specifici in materia di (i) adeguata verifica della clientela, (ii) conservazione dei dati, delle informazioni e dei documenti, (iii) monitoraggio delle transazioni, (iv) segnalazione delle operazioni sospette e (v) gestione del rischio nell'ambito extra SEE;
- svolge il ruolo di indirizzo, coordinamento e controllo nei confronti delle Società controllate non in gestione accentrata e delle Filiali Estere.

Con specifico riferimento agli obblighi di adeguata verifica della clientela, la Direzione Centrale Anti Financial Crime svolge le seguenti attività:

- predispone ed aggiorna le regole e le metodologie e supporta la redazione dei processi operativi inerenti alla identificazione e profilatura del cliente, esecuzione delle attività di adeguata verifica, ordinaria e rafforzata, e armonizzazione dei profili di rischio per la clientela comune all'interno del Gruppo;
- valuta ed autorizza l'apertura di un nuovo rapporto, l'esecuzione di un'operazione occasionale o il mantenimento di un rapporto già in essere per i clienti in fascia di rischio alto, inclusa l'apertura di rapporti di corrispondenza o il mantenimento della relazione già in essere per gli enti creditizi e finanziari in fascia di rischio alto, fatte salve eventuali sub-deleghe attribuite dal Responsabile della Direzione Centrale Anti Financial Crime ad altre strutture della Banca sulla base di criteri oggettivi e predeterminati;
- valuta ed autorizza l'apertura di un nuovo rapporto, l'esecuzione di un'operazione occasionale o il mantenimento di un rapporto già in essere, su posizioni in fascia di rischio medio alto, a fronte di specifica richiesta da parte delle strutture operative, per casistiche specificamente indicate nelle regole metodologiche nonché nel caso in cui il personale incaricato delle attività valutative o autorizzative si trovi in situazioni anche potenziali di conflitto di interessi;
- valuta i nominativi per i quali ci sia stato un riscontro positivo con le Sanction List e/o le liste antiterrorismo, sia in sede di screening anagrafico sia di monitoraggio delle transazioni, qualora individuato dai sistemi di controllo automatici e confermato a seguito delle verifiche effettuate dalla competente struttura della Direzione Centrale Operations;
- predispone e certifica il questionario standard relativo ai processi interni e alle procedure adottati dalla Banca in materia di antiriciclaggio, di contrasto al finanziamento del terrorismo e di gestione degli embarghi da rilasciare, nella generalità dei casi, agli enti creditizi e finanziari che effettuano l'adeguata verifica per l'instaurazione di relazioni di corrispondenza o rapporti assimilati con la Banca.

Con specifico riferimento agli obblighi di conservazione dei dati, delle informazioni e dei documenti, la Direzione Centrale Anti Financial Crime svolge le seguenti attività:

- definisce i requisiti di alimentazione e di gestione dell'archivio di conservazione dei dati per l'adempimento degli obblighi antiriciclaggio ("Archivio Unico Informatico" o "AUI") e verifica l'affidabilità del relativo sistema informativo di alimentazione, basandosi anche sui controlli effettuati dalle altre strutture aziendali. In particolare, la Direzione Centrale Anti Financial Crime

fornisce il proprio supporto nella fase di analisi degli interventi informatici su detto archivio e coordina gli interventi per rimuovere eventuali anomalie riscontrate sulla gestione dello stesso;

- controlla, a campione, la qualità dei dati statistici da inviare all'UIF e coordina le rettifiche, ritenute necessarie, delle informazioni registrate nel relativo archivio, anche a seguito di richiesta da parte delle strutture operative;
- trasmette all'UIF i dati aggregati concernenti le suddette registrazioni.

Con specifico riferimento agli adempimenti previsti in tema di monitoraggio delle operazioni, la Direzione Centrale Anti Financial Crime svolge le seguenti attività:

- presidia i modelli, le metodologie e le metriche di rilevazione per il monitoraggio transazionale in materia di antiriciclaggio, contrasto al terrorismo e gestione degli embarghi e, in particolare, definisce e monitora il corretto funzionamento degli scenari di monitoraggio e delle modalità di screening, ne effettua la definizione dei parametri e la calibrazione degli algoritmi;
- supporta la funzione Compliance Digital Transformation nella mappatura e nell'aggiornamento dei dati alimentanti i sistemi informatici di monitoraggio;
- è responsabile delle attività di secondo livello in materia di antiriciclaggio svolte dal Competence Center di Transaction Monitoring e pertanto:
 - esamina le operazioni anomale intercettate dai sistemi informatici di monitoraggio transazionale e valutate, dal primo livello del Competence Center presso la Direzione Centrale Operations, come meritevoli di approfondimento;
 - qualora risulti necessaria un'integrazione delle analisi, acquisisce le informazioni aggiuntive dal Responsabile della struttura operativa competente e ne valuta i riscontri ricevuti;
 - notifica quindi al Responsabile della struttura operativa competente, in presenza di elementi comprovati di anomalia, la comunicazione per la valutazione dell'avvio dell'iter di segnalazione di operazione sospetta;
 - in caso di operazioni con chiari indizi di sospetto, la comunicazione al Responsabile della struttura operativa avviene tramite le c.d. "riservatissime", normalmente utilizzate ad esito delle attività di controllo, per attivare senza ritardo le valutazioni del caso per l'avvio dell'iter di segnalazione, con contestuale informativa al Responsabile delle segnalazioni di operazioni sospette;
- gestisce le attività inerenti i nominativi, i rapporti e le controparti inseriti nelle c.d. Exemption list e Monitoring list⁴ a seguito dell'approvazione da parte del Tavolo di gestione e supervisione degli scenari di monitoraggio transazionale in materia di antiriciclaggio e/o del Responsabile della Direzione Centrale Anti Financial Crime;
- effettua le valutazioni di competenza sulle transazioni e sulle anagrafiche ai fini della gestione degli embarghi e del contrasto al terrorismo, incluse quelle relative all'operatività in strumenti finanziari, valutando le situazioni riguardanti nominativi risultati positivi ai riscontri con le Sanction List e/o con le liste antiterrorismo, a seguito delle analisi di primo livello effettuate dalle competenti strutture della Direzione Centrale Operations, e assumendo gli opportuni provvedimenti, ivi inclusa la valutazione dell'avvio dell'iter di segnalazione di operazione sospetta tramite la c.d. "riservatissima", nonché effettuando le valutazioni di competenza preventive sulle operazioni connotate da un significativo rischio di non conformità in materia di embarghi;
- definisce e svolge le attività di control testing sui processi secondo il piano annuale di verifica; in particolare, verifica la qualità del processo di analisi delle evidenze presenti nei sistemi e delle operazioni anomale intercettate dai sistemi informatici e valutate come non rilevanti da parte del primo e del secondo livello del Competence Center e valuta l'adeguatezza e la coerenza delle attività agite e delle determinazioni assunte negli approfondimenti rispetto al processo ed alle evidenze disponibili (c.d. "quality assurance");

⁴ L'Exemption list comprende i nominativi, le controparti o i rapporti per i quali viene temporaneamente esclusa, con riferimento a uno o più scenari di monitoraggio, la pubblicazione di alert nei sistemi informatici di monitoraggio transazionale col fine di ridurre l'incidenza di detection/alert ridondanti o di scarsa efficacia. La Monitoring list comprende i nominativi, i rapporti o le controparti che sono oggetto di un monitoraggio più stringente.

- trasmette all'UIF le periodiche comunicazioni oggettive in conformità alle disposizioni di attuazione emanate dall'UIF;
- trasmette all'UIF ed al Nucleo Speciale della Guardia di Finanza le comunicazioni inerenti al congelamento di fondi e risorse economiche riconducibili ai soggetti designati destinatari di misure restrittive nell'ambito della normativa sugli embarghi e sul contrasto al finanziamento del terrorismo.

Con specifico riferimento agli adempimenti previsti in tema di segnalazione delle operazioni sospette, la Direzione Centrale Anti Financial Crime - per il tramite del Responsabile delle segnalazioni di operazioni sospette - svolge le seguenti attività:

- effettua all'UIF le segnalazioni di operazioni sospette di secondo livello in materia di riciclaggio, di finanziamento del terrorismo o di finanziamento di programmi di proliferazione di armi di distruzione di massa, mine antipersona, munizioni e submunizioni a grappolo;
- gestisce gli adempimenti connessi agli accessi dell'Autorità, ed in particolare dell'UIF e della Guardia di Finanza.

Con specifico riferimento al reporting periodico ed ai flussi informativi diretti agli Organi Societari, la Direzione Centrale Anti Financial Crime:

- predispone e presenta, con cadenza di norma annuale, per approvazione al Consiglio di Amministrazione, previo esame del Comitato Rischi e del Comitato per il Controllo sulla Gestione, la programmazione delle attività;
- predispone e presenta, con cadenza semestrale, al Comitato Rischi, al Comitato per il Controllo sulla Gestione e al Consiglio di Amministrazione una relazione sulle attività di verifica svolte, sulle iniziative intraprese, sulle disfunzioni accertate e sulle relative azioni correttive da intraprendere nonché sull'attività formativa del personale;
- analizza le rilevazioni delle infrazioni gravi, o ripetute o sistematiche o plurime ai sensi dell'art. 46, comma 1, lett. b) e delle infrazioni ai sensi dell'art. 51, comma 1, del D. Lgs. n. 231/2007, pervenute dal Chief Audit Officer o da altre funzioni aziendali o autonomamente individuate e fornisce la relativa informativa, con periodicità semestrale, al Comitato per il Controllo sulla Gestione; in caso di infrazioni di particolare gravità tale informativa viene fornita alla prima riunione utile per consentire la tempestiva comunicazione all'Autorità di Vigilanza o al MEF;
- prende visione delle comunicazioni ai sensi degli articoli 46 e 51 del D. Lgs. n. 231/2007, inoltrate all'Autorità di Vigilanza, al MEF o al Responsabile delle segnalazioni di operazioni sospette da parte del Comitato per il Controllo sulla Gestione e relaziona a quest'ultimo circa le azioni correttive intraprese.

Con specifico riferimento alla formazione del personale, la Direzione Centrale Anti Financial Crime svolge le seguenti attività:

- individua gli obiettivi formativi e predispone un adeguato piano di formazione finalizzato a conseguire un costante aggiornamento del personale dipendente, in collaborazione con la Direzione Centrale Compliance Governance e Controlli, con la Direzione Centrale Politiche di Sviluppo e Learning Academy, con la Direzione Centrale People Management & HR Transformation, con le strutture HR delle Divisioni e con la Comunicazione Interna;
- definisce i contenuti degli interventi formativi previsti e supporta la Direzione Centrale Politiche di Sviluppo e Learning Academy, la Direzione Centrale People Management & HR Transformation e le strutture HR delle Divisioni nella definizione delle modalità di erogazione degli stessi.

Nell'ambito della Direzione Centrale Anti Financial Crime sono attribuiti al Responsabile della Direzione Centrale Anti Financial Crime:

- il ruolo di Responsabile della Funzione Antiriciclaggio;
- il ruolo di Referente S.AR.A. (Segnalazioni AntiRiciclaggio Aggregate).

3.3.1.1 Responsabile della Funzione Antiriciclaggio

Il ruolo di Responsabile della Funzione Antiriciclaggio è attribuito al Responsabile della Direzione Centrale Anti Financial Crime, che viene nominato dal Consiglio di Amministrazione, con il supporto del Comitato Rischi, sentito il Comitato per il Controllo sulla Gestione.

Il Responsabile della Direzione Centrale Anti Financial Crime:

- deve essere in possesso di requisiti di idoneità previsti dalla normativa⁵ e di adeguati requisiti di indipendenza, autorevolezza e professionalità e non deve avere responsabilità dirette di aree operative né deve essere gerarchicamente dipendente da soggetti responsabili di dette aree;
- rientra, a tutti gli effetti, nel novero dei responsabili di funzioni aziendali di controllo ed è indipendente nell'esecuzione delle proprie funzioni;
- riceve dai Responsabili delle segnalazioni di operazioni sospette delle Società del Gruppo un flusso informativo periodico relativo alle segnalazioni inoltrate e archiviate e può richiedere di prendere visione delle segnalazioni inoltrate e di quelle archiviate⁶;
- svolge un ruolo di supervisione sull'adeguatezza dell'organizzazione delle attività e dell'effettiva attuazione dei processi e delle procedure interne in materia di antiriciclaggio, di contrasto al finanziamento del terrorismo e di gestione degli embarghi nell'ambito di tutte le strutture aziendali, anche se tali strutture non appartengono alla Direzione Centrale Anti Financial Crime. Nello svolgimento di tale ruolo e per i profili di competenza, condivide con le competenti strutture delle funzioni operative e di supporto le attività di controllo di primo livello da effettuare e le modalità di attuazione delle stesse;
- si avvale degli esiti delle attività di controllo di secondo livello svolte dalle competenti strutture appartenenti alla propria Direzione e alla Direzione Centrale Compliance Governance e Controlli, nonché delle evidenze che emergono dalle attività di verifica condotte dalle strutture del Chief Audit Officer nella sua funzione di controllo indipendente di terzo livello;
- verifica l'adeguatezza dei processi e delle procedure interne in materia di rilevazione, valutazione e segnalazione delle operazioni sospette in quanto responsabile del monitoraggio dell'efficacia di tutto il sistema di gestione e di quello dei controlli interni a presidio del rischio di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi;
- viene supportato dal Tavolo di gestione e supervisione degli scenari per garantire l'adeguatezza, l'efficacia degli scenari di monitoraggio transazionale e indirizzarne i relativi processi di modifica del perimetro di applicazione.

Il Responsabile della Direzione Centrale Anti Financial Crime riveste anche il ruolo di Responsabile Antiriciclaggio per le principali Società del Gruppo in cui è prevista l'applicazione del modello di gestione accentrata e, in considerazione del ruolo di indirizzo, coordinamento e controllo della Capogruppo nei confronti delle Società del Gruppo, assume altresì il ruolo di Responsabile Antiriciclaggio di Gruppo, cui viene ricondotta la gestione complessiva del rischio di riciclaggio a livello di Gruppo.

Al Responsabile della Direzione Centrale Anti Financial Crime è rilasciata dal Consigliere Delegato e CEO, in qualità di Direttore Generale, la delega per l'autorizzazione all'apertura di rapporti transfrontalieri con enti creditizi e finanziari corrispondenti di un Paese extra SEE, per l'autorizzazione all'instaurazione/mantenimento di rapporti continuativi o al compimento di operazioni occasionali con Persone Politicamente Esposte ("PEP"), nazionali ed estere, e per l'instaurazione/mantenimento di rapporti continuativi o al compimento di operazioni occasionali che coinvolgono Paesi ad alto rischio, fatte salve le ulteriori deleghe attribuite dal Consigliere Delegato e CEO ad altre strutture della Banca.

⁵ In particolare, l'Organo con funzione di supervisione strategica valuta, preventivamente alla nomina, il possesso dei requisiti previsti dalla normativa di vigilanza e, fatti salvi i casi di urgenza, trasmette il relativo verbale all'Autorità di Vigilanza competente.

⁶ La circolazione delle informazioni analitiche sulle segnalazioni inoltrate alle FIU (Financial Intelligence Unit) locali ha luogo salvo eventuali impedimenti prescritti dall'ordinamento giuridico del Paese in cui ha sede la Società.

Il Responsabile della Direzione Centrale Anti Financial Crime riporta direttamente al Responsabile dell'Area di Governo Chief Compliance Officer.

3.3.1.2 Responsabile delle segnalazioni di operazioni sospette

Il Responsabile delle segnalazioni di operazioni sospette viene nominato dal Consiglio di Amministrazione, sentito il Comitato per il Controllo sulla Gestione.

Il Responsabile delle segnalazioni di operazioni sospette:

- deve essere in possesso di adeguati requisiti di indipendenza, autorevolezza e professionalità e non deve avere responsabilità dirette di aree operative né deve essere gerarchicamente dipendente da soggetti responsabili di dette aree;
- è indipendente nell'esercizio delle sue funzioni;
- può coincidere con il Responsabile della Funzione Antiriciclaggio; in caso di non coincidenza può acquisire dal Responsabile della Funzione Antiriciclaggio informazioni utili al processo di valutazione delle operazioni sospette;
- riveste anche il ruolo di Delegato di Gruppo, con l'attribuzione della delega per l'inoltro all'UIF delle segnalazioni di operazioni sospette anche per le Società del Gruppo per le quali è prevista l'applicazione del modello di gestione accentrata;
- ha libero accesso ai flussi informativi diretti agli Organi Societari e alle strutture coinvolte nelle attività di contrasto del riciclaggio e del finanziamento del terrorismo;
- può consentire, con le indispensabili cautele di riservatezza e senza menzionare il nominativo del segnalante, che i Responsabili delle strutture aziendali abbiano conoscenza dei nominativi dei clienti segnalati, considerata la particolare pregnanza che tale informazione può rivestire per l'accettazione di nuovi clienti o per la valutazione dell'operatività di clienti con i quali sia già in essere un rapporto;
- fornisce consulenza alle strutture operative in merito agli adempimenti inerenti alla predisposizione delle segnalazioni di operazioni sospette e all'eventuale astensione dal compimento delle operazioni;
- valuta le segnalazioni di operazioni sospette pervenutegli dalle strutture operative nonché le comunicazioni inoltrate ai sensi dell'art. 46, comma 1, lett. a) del D. Lgs. n. 231/2007 dal Comitato per il Controllo sulla Gestione e predispone la relativa istruttoria;
- trasmette all'UIF le segnalazioni ritenute fondate e archivia, con propria motivazione scritta, le segnalazioni ritenute non fondate;
- comunica l'esito della propria valutazione al Responsabile della struttura operativa che ha proposto la segnalazione;
- comunica al Responsabile della struttura operativa, che aveva proposto la segnalazione di operazione sospetta, l'intervenuta archiviazione della segnalazione disposta dall'UIF, quando ne venga a conoscenza;
- interloquisce con l'UIF e gestisce le richieste di approfondimenti formulate dalle competenti Autorità⁷;
- contribuisce all'individuazione delle misure necessarie a garantire la riservatezza e la conservazione dei dati, delle informazioni e della documentazione relativa alle segnalazioni da sottoporre all'approvazione del Consigliere Delegato e CEO;
- fornisce al Responsabile delle segnalazioni di operazioni sospette delle imprese assicurative per le quali la Banca svolge il ruolo di intermediario assicurativo, le comunicazioni dovute ai

⁷ Con il termine Autorità si fa riferimento a Organi istituzionali quali, ad esempio, la Magistratura, la Guardia di Finanza e il Nucleo speciale di Polizia Valutaria che possono essere coinvolti nelle fasi di investigazione e di approfondimento a seguito di segnalazioni di operazioni sospette provenienti dal sistema finanziario.

sensi del Regolamento IVASS n. 44/2019 come modificato dal Provvedimento IVASS n. 111 del 13/07/2021⁸.

Il Responsabile delle segnalazioni di operazioni sospette, nell'espletamento delle proprie funzioni, si avvale delle strutture preposte della Direzione Centrale Anti Financial Crime; in particolare, può abilitare gli addetti di tali strutture ad operare, sotto la propria responsabilità, nell'ambito del sistema di segnalazione delle operazioni sospette in ottemperanza alle disposizioni impartite dall'UIF.

3.3.1.3 Referente S.AR.A. (Segnalazioni AntiRiciclaggio Aggregate)

Il ruolo di Referente S.AR.A.⁹ è attribuito al Responsabile della Funzione Antiriciclaggio.

Il Referente S.AR.A.:

- è responsabile della trasmissione all'UIF, con cadenza mensile, dei dati aggregati concernenti l'operatività della Banca;
- rappresenta l'interlocutore dell'UIF per tutte le questioni attinenti alle segnalazioni aggregate;
- verifica il corretto funzionamento del sistema informativo interno per la produzione delle segnalazioni;
- può abilitare altri soggetti all'inserimento e alla trasmissione dei dati aggregati.

Il Referente S.AR.A., nell'espletamento delle proprie funzioni, si avvale delle strutture preposte della Direzione Centrale Anti Financial Crime.

3.3.1.4 Tavolo di gestione e supervisione degli scenari

Il Tavolo di gestione e supervisione degli scenari ha un ruolo istruttorio, a supporto del Responsabile della Direzione Centrale Anti Financial Crime, nell'obiettivo di supervisionare il funzionamento degli scenari di monitoraggio transazionale in materia di antiriciclaggio e di garantire una corretta gestione e tracciatura del processo adottato per apportare eventuali modifiche al perimetro di applicazione, regolando le modalità attraverso le quali valutare, testare, validare e tracciare tali modifiche.

Il Tavolo ha il compito di:

- valutare l'adozione, la periodica revisione e l'implementazione degli scenari adottati e della relativa calibrazione tecnica; gli scenari sono sottoposti a revisione, con frequenza annuale e secondo un approccio risk based in termini di entità/scenari;
- valutare l'adozione, la revisione con cadenza almeno annuale e l'implementazione delle Exemption list e Monitoring list¹⁰;
- indirizzare eventuali tematiche funzionali che emergono da problemi tecnici collegati a problemi nell'alimentazione degli scenari, a modifiche delle fonti alimentanti o errori nell'elaborazione degli scenari segnalati dalle fabbriche IT e/o derivanti dall'ordinaria supervisione sulle grandezze/evidenze dei fenomeni sorvegliati;
- supervisionare l'efficacia degli scenari di monitoraggio transazionale e indirizzarne i relativi processi di modifica;
- valutare le eventuali iniziative formative da attivare in materia di scenari di monitoraggio transazionale anche a seguito della previsione di nuovi red flag e/o di nuovi scenari.

⁸ Il Regolamento prevede l'invio all'impresa assicurativa di riferimento delle segnalazioni di operazioni sospette riferite alle "stesse operazioni" già segnalate direttamente alla UIF e di dare notizia all'impresa dell'avvenuta segnalazione di uno "stesso cliente".

⁹ Con riferimento alle società estere del Gruppo, la previsione si applica solo se analogo ruolo è previsto dalla normativa nazionale di riferimento e con le modalità da essa definite.

¹⁰ Il Tavolo è tenuto a valutare le proposte di adozione e implementazione dell'Exemption list formulate dalle Filiali estere ed è informato, con cadenza mensile, delle variazioni apportate in autonomia dalle Filiali estere alla Monitoring list e ha facoltà di richiedere l'aggiunta di un nominativo alla lista.

3.3.2 Direzione Centrale Compliance Governance e Controlli

I compiti e le responsabilità della Direzione Centrale Compliance Governance e Controlli sono descritti nel “Funzionigramma della struttura”.

Con riferimento alle tematiche relative all’antiriciclaggio, al contrasto al finanziamento del terrorismo ed alla gestione degli embarghi, la Direzione Centrale Compliance Governance e Controlli supporta la Direzione Centrale Anti Financial Crime assicurando:

- l’attività di controllo di secondo livello per la Capogruppo e le Società controllate in gestione accentrata;
- l’attività di elaborazione degli indicatori di monitoraggio delle fenomenologie a maggiore rischio individuati di concerto con la Direzione Centrale Anti Financial Crime;
- lo sviluppo delle metodologie di AFC Risk Assessment ed il monitoraggio degli interventi di formazione attuati sulle Banche e Società in gestione accentrata.

In relazione alle proprie attività di controllo, la Direzione Centrale Compliance Governance e Controlli:

- individua le ipotesi di infrazioni gravi o ripetute o sistematiche o plurime ai sensi dell’art. 46, comma 1, lett. b) e le ipotesi dell’art. 51, comma 1 del D. Lgs. n. 231/2007 e le segnala alla Direzione Centrale Anti Financial Crime per l’ulteriore analisi, da parte di quest’ultima, prima dell’inoltro della relativa comunicazione al Comitato per il Controllo sulla Gestione;
- trasmette al Responsabile della struttura operativa, ai sensi dell’art. 46, comma 1, lett. a), la comunicazione c.d. “riservatissima” per attivare senza ritardo le valutazioni del caso per l’avvio dell’iter di segnalazione delle operazioni individuate come potenzialmente sospette. Di ciò informa contestualmente il Responsabile delle segnalazioni di operazioni sospette.

3.3.3 Compliance Digital Transformation

I compiti e le responsabilità della struttura Compliance Digital Transformation sono descritti nel “Funzionigramma della struttura”.

Con riferimento alle tematiche relative all’antiriciclaggio, al contrasto al finanziamento del terrorismo e alla gestione degli embarghi, la struttura:

- svolge il ruolo di Data Owner per i sotto domini assegnati all’Area di Governo Chief Compliance Officer, coordinandosi con le strutture competenti della Direzione Centrale Anti Financial Crime, Direzione Centrale Data Office, Data technology Owner, Data Owner e Data Technology Owner degli applicativi impattati al fine di garantire la corretta implementazione del feeding richiesto da Direzione Centrale Anti Financial Crime;
- contribuisce, con il supporto delle competenti funzioni previste dal framework aziendale di Data Governance, a garantire la qualità dei dati in ambito antiriciclaggio, presidiando e/o attuando, ove necessario, i controlli definiti. In tale ambito la struttura agisce il ruolo di Data Owner relativamente alle elaborazioni dei dati ai fini del monitoraggio transazionale; a tal fine:
 - gestisce tempestivamente, con il supporto delle strutture previste nelle Linee Guida in materia di Data Governance, gli errori e gli scarti che dovessero emergere in fase di impianto nonché nel corso della gestione nel continuo del sistema informatico;
 - supporta la Direzione Centrale Anti Financial Crime d’intesa con le altre funzioni competenti nello sviluppo di soluzioni tecnologiche volte a migliorare l’efficacia e l’efficienza del modello di Transaction Monitoring e screening.

3.4 Area di Governo Chief Risk Officer

I compiti e le responsabilità dell’Area di Governo Chief Risk Officer e delle strutture a suo diretto riporto sono descritti nei “Funzionigrammi della strutture” e nel “Regolamento SCII”.

Con riferimento alle tematiche relative all'antiriciclaggio, al contrasto al finanziamento del terrorismo ed alla gestione degli embarghi, l'Area di Governo Chief Risk Officer svolge le seguenti attività:

- collabora con il Responsabile della Direzione Centrale Anti Financial Crime, che opera d'intesa con il Responsabile dell'Area di Governo Chief Compliance Officer, per la definizione delle metodologie di AFC Risk Assessment favorendo le sinergie con gli strumenti e i metodi propri dell'Operational Risk Management;
- collabora con il Responsabile della Direzione Centrale Anti Financial Crime, che opera d'intesa con il Responsabile dell'Area di Governo Chief Compliance Officer, per integrare il modello di valutazione e gestione del rischio di non conformità nel RAF;
- supporta le strutture dell'Area di Governo Chief Compliance Officer nella valutazione della conformità alla normativa vigente delle operazioni e dei nuovi prodotti e servizi da avviare alla commercializzazione, anche con riferimento all'ingresso in nuove attività e nuovi mercati, sia su richiesta sia attraverso processi strutturati di Product Governance e di clearing, collaborando nell'identificazione dei rischi potenziali per la Banca e per i clienti e fornendo, ove applicabili, valutazioni quantitative;
- procede, con frequenza e modalità definite secondo le "Regole di Validazione" secondo un approccio risk based e anche con il supporto esterno di esperti del settore, alla validazione indipendente dei modelli interni sviluppati in ambito monitoraggio transazionale in materia di antiriciclaggio, contrasto al terrorismo e gestione degli embarghi e per i quali è stata identificata come model reviewer.

Le modalità di collaborazione tra le Aree di Governo Chief Risk Officer e Chief Compliance Officer e i relativi scambi di flussi informativi sono declinati all'interno del "Regolamento SCII".

3.5 Chief Audit Officer

Il Chief Audit Officer assicura una costante e indipendente azione di sorveglianza sul regolare andamento dell'operatività e dei processi della Banca e del Gruppo al fine di prevenire o rilevare l'insorgere di comportamenti o situazioni anomale e rischiose, valutando la funzionalità del sistema dei controlli interni e la sua idoneità a garantire l'efficacia e l'efficienza dei processi aziendali, la salvaguardia del valore delle attività e la protezione dalle perdite, l'affidabilità e l'integrità delle informazioni contabili e gestionali, la conformità delle operazioni alle politiche stabilite dagli Organi di governo aziendali e alle normative interne ed esterne.

Con riferimento alle tematiche relative all'antiriciclaggio, al contrasto al finanziamento del terrorismo ed alla gestione degli embarghi, il Chief Audit Officer, nell'ambito della propria attività di presidio di terzo livello del complessivo sistema dei controlli interni, verifica in modo continuativo il grado di adeguatezza dell'assetto organizzativo aziendale nonché la sua conformità rispetto alla disciplina di riferimento e vigila sulla funzionalità (in termini di efficienza ed efficacia) e l'affidabilità del modello di Gruppo di gestione dei rischi di cui sopra. In particolare, il Chief Audit Officer sottopone a verifica periodica l'adeguatezza e l'efficacia della Direzione Centrale Anti Financial Crime e fornisce l'esito delle sue valutazioni nell'ambito dei consueti flussi informativi diretti agli Organi Societari competenti. Il Chief Audit Officer, nell'ambito della propria attività di presidio, verifica tra l'altro:

- il costante rispetto degli adempimenti di adeguata verifica, sia nella fase di instaurazione del rapporto che nel corso della relazione con il cliente;
- l'effettiva acquisizione e l'ordinata conservazione dei dati, delle informazioni e dei documenti previsti dalla normativa di riferimento;
- il corretto funzionamento dell'archivio di conservazione dei dati delle operazioni poste in essere dalla clientela;
- l'effettiva responsabilizzazione del personale dipendente e dei collaboratori nonché dei responsabili delle strutture centrali e periferiche nell'espletamento di tutti gli adempimenti previsti dalla normativa di riferimento.

Inoltre, il Chief Audit Officer:

- predisporre, sulla base delle risultanze dell’Audit Risk Assessment e dei controlli effettuati dalle competenti funzioni di primo e secondo livello, il piano dei controlli su tutte le strutture operative coinvolte; ciò allo scopo di garantire un presidio rafforzato sulle strutture maggiormente esposte ai rischi di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi;
- verifica, in occasione degli interventi di audit, l’allineamento tra le varie procedure contabili di gestione delle operazioni poste in essere dalla clientela e la procedura di alimentazione e gestione dell’archivio di conservazione dei dati previsto dalla normativa antiriciclaggio;
- segnala alla Direzione Centrale Anti Financial Crime ed agli Organi Societari competenti le inefficienze riscontrate nel corso dell’attività di verifica e suggerisce i correttivi da apportare;
- svolge interventi di “*follow up*” per verificare l’intervenuta adozione delle necessarie azioni correttive e la loro idoneità a evitare analoghe situazioni di criticità nel futuro.

A seguito dei controlli e delle valutazioni effettuate, il Chief Audit Officer:

- individua le ipotesi di infrazioni gravi o ripetute o sistematiche o plurime ai sensi dell’art. 46, comma 1, lett. b) e le ipotesi dell’art. 51, comma 1 del D. Lgs. n. 231/2007 e le segnala alla Direzione Centrale Anti Financial Crime per l’ulteriore analisi, da parte di quest’ultima, prima dell’inoltro della relativa comunicazione al Comitato per il Controllo sulla Gestione;
- trasmette al Responsabile della struttura operativa, ai sensi dell’art. 46, comma 1, lett. a), la comunicazione c.d. “riservatissima” per attivare senza ritardo le valutazioni del caso per l’avvio dell’iter di segnalazione delle operazioni individuate come potenzialmente sospette. Di ciò informa contestualmente il Responsabile delle segnalazioni di operazioni sospette.

3.6 Area di Governo Chief Operating Officer

3.6.1 Direzione Centrale Organizzazione

I compiti e le responsabilità della Direzione Centrale Organizzazione sono descritti nel “Funzionigramma della struttura”.

La Direzione Centrale Organizzazione svolge le seguenti attività:

- definisce soluzioni organizzative coerenti con gli obiettivi e gli indirizzi previsti in materia di antiriciclaggio, di contrasto al finanziamento del terrorismo e di gestione degli embarghi, avvalendosi della consulenza e della collaborazione della Direzione Centrale Anti Financial Crime;
- verifica e definisce, con l’approvazione del Responsabile dell’Area di Governo Chief Operating Officer, il dimensionamento quantitativo degli organici in coerenza con gli obiettivi e gli indirizzi dei piani aziendali;
- supporta la Direzione Centrale Anti Financial Crime nell’aggiornamento della documentazione di governance, declinando ruoli e responsabilità previsti;
- presidia la diffusione della normativa interna e della documentazione di governance della Banca in materia di antiriciclaggio, di contrasto al finanziamento del terrorismo e di gestione degli embarghi.

In particolare, la Direzione Centrale Organizzazione presidia l’analisi e l’adozione di interventi organizzativi, anche derivanti da nuovi adempimenti normativi. Inoltre, procede, secondo logiche di priorità, all’aggiornamento delle analisi di dimensionamento funzionali alla programmazione annuale delle attività della Direzione Centrale Anti Financial Crime.

3.6.2 Direzione Centrale Politiche di Sviluppo e Learning Academy

I compiti e le responsabilità della Direzione Centrale Politiche di Sviluppo e Learning Academy sono descritti nel “Funzionigramma della struttura”.

Con riferimento alle tematiche relative all'antiriciclaggio, al contrasto al finanziamento del terrorismo ed alla gestione degli embarghi, la Direzione Centrale Politiche di Sviluppo e Learning Academy svolge le seguenti attività:

- concorre, con le strutture dell'Area di Governo Chief Compliance Officer ed in particolare con la Direzione Centrale Anti Financial Crime, allo sviluppo di iniziative finalizzate a diffondere, a tutti i livelli aziendali, una cultura aziendale coerente con i principi di conformità alle norme e ad ampliare il livello di consapevolezza dell'approccio al rischio richiesto;
- collabora con la Direzione Centrale People Management & HR Transformation e con le funzioni HR delle diverse Divisioni per l'attuazione degli interventi formativi sugli ambiti di conformità, con il supporto delle strutture dell'Area di Governo Chief Compliance Officer ed in particolare con la Direzione Centrale Anti Financial Crime, che ne predispongono i contenuti, e con Comunicazione Interna, per l'attivazione di canali di comunicazione efficaci per la diffusione all'interno dell'azienda della cultura in materia di compliance;
- collabora con la Direzione Centrale People Management & HR Transformation, con le funzioni HR delle diverse Divisioni e con le strutture dell'Area di Governo Chief Compliance Officer ed in particolare con la Direzione Centrale Anti Financial Crime per la definizione e realizzazione di programmi di formazione nel continuo finalizzati al potenziamento delle competenze tecnico-professionali e all'aggiornamento del personale addetto alle attività di compliance.

3.6.3 Direzione Centrale People Management & HR Transformation

I compiti e le responsabilità della Direzione Centrale People Management & HR Transformation sono descritti nel "Funzionigramma della struttura".

Con riferimento alle tematiche relative all'antiriciclaggio, al contrasto al finanziamento del terrorismo ed alla gestione degli embarghi la Direzione Centrale People Management & HR Transformation e le funzioni HR delle diverse Divisioni assicurano la corretta copertura quali-quantitativa degli organici necessari per assolvere gli adempimenti previsti dalla normativa e collaborano con la Direzione Centrale Politiche di Sviluppo e Learning Academy per l'attuazione degli interventi formativi sugli ambiti di conformità, con il supporto delle strutture dell'Area di Governo Chief Compliance Officer ed in particolare con la Direzione Centrale Anti Financial Crime.

3.6.4 Direzione Centrale Affari Sindacali e Politiche del Lavoro

I compiti e le responsabilità della Direzione Centrale Affari Sindacali e Politiche del Lavoro sono descritti nel "Funzionigramma della struttura".

Con riferimento alle tematiche relative all'antiriciclaggio, al contrasto al finanziamento del terrorismo ed alla gestione degli embarghi, la Direzione Centrale Affari Sindacali e Politiche del Lavoro:

- valuta e cura azioni disciplinari nei confronti di dipendenti per i quali siano state rilevate violazioni delle normative;
- valuta l'applicabilità delle tutele previste dalla contrattazione collettiva ai dipendenti coinvolti in procedimenti penali, civili e amministrativi per presunte violazioni delle normative di riferimento e decide sulla formulazione delle riserve da sciogliere in sede di definizione del giudizio.

3.7 Area di Governo Chief IT, Digital and Innovation Officer

3.7.1 Transformation Center

I compiti e le responsabilità del Transformation Center sono descritti nel "Funzionigramma della struttura".

Con riferimento alle tematiche relative all'antiriciclaggio, al contrasto al finanziamento del terrorismo ed alla gestione degli embarghi, il Transformation Center svolge le seguenti attività:

- supporta il process owner nella progettazione dei processi aziendali e il presidio dell'aggiornamento e della pubblicazione della normativa interna in materia di antiriciclaggio, di contrasto al finanziamento del terrorismo e di gestione degli embarghi;
- individua, di concerto con la Direzione Centrale Anti Financial Crime e le funzioni interessate, i requisiti per lo sviluppo delle soluzioni informatiche più idonee alla semplificazione e all'efficientamento dei processi di competenza.

3.7.2 Direzione Centrale Operations

I compiti e le responsabilità della Direzione Centrale Operations sono descritti nel “Funzionigramma della struttura”.

Con riferimento alle tematiche relative all'antiriciclaggio, al contrasto al finanziamento del terrorismo ed alla gestione degli embarghi, la Direzione Centrale Operations svolge le seguenti attività:

- effettua controlli di primo livello sulla qualità dei dati che alimentano l'archivio di conservazione dei dati, indirizzando alla Direzione Centrale Sistemi Informativi le richieste di eventuali interventi correttivi e garantendo un flusso informativo periodico verso la Direzione Centrale Anti Financial Crime con il dettaglio delle anomalie riscontrate e dell'avanzamento degli interventi correttivi posti in essere;
- verifica, sulla base di regole definite dalla Direzione Centrale Anti Financial Crime, i riscontri positivi alle Sanction List e/o alle liste interne a fini antiterrorismo ed embarghi derivanti da un sistema automatico di filtraggio e coinvolge la Direzione Centrale Anti Financial Crime nei casi dubbi e/o di conferma del sospetto;
- effettua, applicando le regole definite dalla Direzione Centrale Anti Financial Crime, i controlli sui pagamenti e sui documenti rappresentativi di merci in caso di riscontro positivo con le Sanction List e/o alle liste interne a fini antiterrorismo ed embarghi, coinvolgendo la Direzione Centrale Anti Financial Crime nei casi dubbi e/o di conferma del sospetto;
- effettua, sulla base di regole definite dalla Direzione Centrale Anti Financial Crime, i controlli sui trasferimenti di fondi finalizzati a garantire la conformità alle previsioni contenute nel Regolamento UE 2015/847, riguardante i dati informativi che accompagnano i trasferimenti di fondi;
- è responsabile delle attività di primo livello svolte dal Competence Center di Transaction Monitoring e pertanto analizza le operazioni anomale evidenziate dalle procedure di monitoraggio transazionale e provvede, all'esito delle verifiche, a: (i) archiviare l'operazione, nel caso in cui si tratti di un falso positivo, non essendo configurabili elementi di anomalia, o non ravvisi motivazioni per inoltrare l'operazione alla Direzione Centrale Anti Financial Crime, (ii) coinvolgere la Direzione Centrale Anti Financial Crime, in presenza di profili di anomalia o necessità di approfondimenti; per la sola operatività di “tramitazione” o “pass through”¹¹ acquisisce presso le strutture esterne competenti le informazioni aggiuntive necessarie per la valutazione dell'operatività oggetto di analisi; propone inoltre i clienti, i rapporti e le controparti da includere/cancellare nella Exemption list;
- inoltra al MEF le comunicazioni inerenti le infrazioni alla normativa in tema di limitazioni all'uso del denaro contante e dei titoli al portatore individuate dalle strutture operative delle Divisioni.

3.7.3 Digital Business Partner

I compiti e le responsabilità di Digital Business Partner sono descritti nel “Funzionigramma della struttura”.

Con riferimento alle tematiche relative all'antiriciclaggio, al contrasto al finanziamento del terrorismo ed alla gestione degli embarghi, Digital Business Partner collabora, in base ai requisiti richiesti dalla

¹¹ Trattasi delle operazioni di pagamento provenienti da altri enti creditizi e finanziari, avvenute con il coinvolgimento di Intesa Sanpaolo quale prestatore del servizio e dirette verso altri enti.

Direzione Centrale Anti Financial Crime, nel coordinamento delle richieste alla Direzione Centrale Sistemi Informativi finalizzate ad effettuare interventi sui sistemi informatici.

3.7.4 Direzione Centrale Sistemi Informativi

I compiti e le responsabilità della Direzione Centrale Sistemi Informativi sono descritti nel “Funzionigramma della struttura”.

Con riferimento alle tematiche relative all’antiriciclaggio, al contrasto al finanziamento del terrorismo ed alla gestione degli embarghi, la Direzione Centrale Sistemi Informativi è coinvolta nello sviluppo, nell’aggiornamento e nel presidio delle componenti applicative e, a tal fine, svolge le seguenti attività:

- implementa e manutiene, in base ai requisiti definiti dalla Direzione Centrale Anti Financial Crime, i sistemi informatici utilizzati per lo svolgimento degli adempimenti in materia;
- controlla l’integrità e completezza tecnica dei flussi che alimentano le diverse soluzioni applicative utilizzate, con particolare riferimento all’archivio di conservazione dei dati per l’adempimento degli obblighi antiriciclaggio (AUI). In caso di anomalie tecniche, la Direzione Centrale Sistemi Informativi provvede ad attivare i necessari interventi correttivi e ne informa la Direzione Centrale Anti Financial Crime; in caso di anomalie che presentano risvolti funzionali e/o normativi, la Direzione Centrale Sistemi Informativi analizza e definisce gli interventi correttivi in collaborazione con la Direzione Centrale Anti Financial Crime;
- partecipa al processo di trasformazione e alla definizione dei controlli tecnici formali dei dati al fine di garantire la corretta alimentazione del tracciato di input ai sistemi informatici utilizzati nel processo di monitoraggio transazionale;
- agisce il ruolo di Data Technology Owner e Data Technology Office in aderenza alle Linee guida in materia di Data Governance;
- aggiorna, di concerto con la Direzione Centrale Anti Financial Crime, le Sanction List, le liste antiterrorismo e gli standard di controllo applicati;
- evade le richieste di interventi evolutivi e correttivi sui sistemi informatici, provenienti dalla Direzione Centrale Anti Financial Crime e dal Chief Audit Officer, dalla funzione Compliance Digital Transformation e dalla Direzione Centrale Operations come concertati, per l’ambito antiriciclaggio, con la Direzione Centrale Anti Financial Crime.

3.7.5 Direzione Centrale Cybersecurity and Business Continuity Management

I compiti e le responsabilità della Direzione Centrale Cybersecurity and Business Continuity Management sono descritti nel “Funzionigramma della struttura”.

La struttura definisce le regole e gli interventi per la tutela di dati, informazioni e infrastrutture per garantire la continuità operativa e il regolare svolgimento delle attività aziendali e per mantenere condizioni di sicurezza allineate alle normative vigenti anche con riferimento ai presidi in materia di antiriciclaggio, contrasto al finanziamento del terrorismo e di gestione degli embarghi.

3.7.6 Direzione Centrale Data Office

I compiti e le responsabilità della Direzione Centrale Data Office sono descritti nel “Funzionigramma della struttura”.

La struttura partecipa all’identificazione dei dati su DSH (Data Service Hub), supportando ove necessario la Direzione Centrale Anti Financial Crime nella declinazione dei requisiti e cooperando con Data Owner e Data Technology Owner dei domini impattati nelle analisi utili all’alimentazione dei dati elementari necessari al corretto funzionamento del sistema informatico. In tale ambito la Direzione svolge un ruolo di supporto alle strutture dei Data Owner e dei Data Technology Owner degli applicativi impattati nello svolgere le attività di decodifica dati, sulla base dei requisiti previamente definiti a cura della Direzione Centrale Anti Financial Crime.

La Direzione partecipa su tutto il processo alle attività di supporto alla funzione Compliance Digital Transformation nell'applicazione del framework di data governance ai fini del monitoraggio transazionale.

3.8 Area di Governo Chief Governance Officer

3.8.1 Direzione Centrale Legale e Contenzioso – Group General Counsel

I compiti e le responsabilità della Direzione Centrale Legale e Contenzioso – Group General Counsel sono descritti nel “Funzionigramma della struttura”.

Con riferimento alle tematiche relative all'antiriciclaggio, al contrasto al finanziamento del terrorismo ed alla gestione degli embarghi, la Direzione Centrale Legale e Contenzioso – Group General Counsel svolge le seguenti attività:

- supporta la Direzione Centrale Anti Financial Crime nella costante individuazione delle norme applicabili monitorandone l'evoluzione, anche giurisprudenziale, e fornisce la propria consulenza per assicurarne la corretta e univoca interpretazione nell'ambito del Gruppo;
- condivide, per i profili giuridici di competenza, i contenuti delle presenti Linee Guida, delle disposizioni normative interne e dei corsi di formazione predisposti dalla Direzione Centrale Anti Financial Crime e dalle altre strutture preposte, formulando proposte di modifica e/o integrazioni;
- fornisce consulenza e assistenza alla Direzione Centrale Anti Financial Crime in merito agli aspetti giuridici controversi attinenti all'esame di conformità dei processi e delle procedure interne, dei contratti, della modulistica o ai casi significativi di disfunzioni rilevate;
- condivide con la Direzione Centrale Anti Financial Crime i testi standard delle comunicazioni da inviare alla clientela in materia di rifiuto all'apertura o all'interruzione di rapporti e di rifiuto all'esecuzione di operazioni occasionali;
- fornisce supporto consulenziale alla Direzione Centrale Anti Financial Crime per valutare preventivamente la conformità dei progetti innovativi, delle operazioni e dei nuovi prodotti e servizi da avviare alla commercializzazione, anche con riferimento all'ingresso in nuove attività o in nuovi mercati.

Le strutture Contenzioso Penale, Amministrativo e Crisi di Impresa e Contenzioso Civile nonché Legale Internazionale, ciascuno per il proprio ambito di competenza, gestiscono le pratiche di precontenzioso e di contenzioso connesse alle violazioni in materia di riciclaggio, di finanziamento del terrorismo e di embarghi.

3.9 Area di Governo Chief Institutional Affairs and External Communication Officer

3.9.1 Direzione Centrale Institutional Affairs e struttura International Public Affairs

I compiti e le responsabilità della Direzione Centrale Institutional Affairs e della struttura International Public Affairs sono descritti nei relativi “Funzionigrammi di struttura”.

Con riferimento alla gestione del rischio di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi, la Direzione Centrale Institutional Affairs e la struttura International Public Affairs monitorano l'evoluzione della normativa, informando le strutture interne e coordinando la risposta del Gruppo alla discussione in merito alle proposte di regolamentazione.

3.10 Divisioni

I compiti e le responsabilità delle Divisioni sono descritti nei relativi “Funzionigrammi di struttura”.

Le Divisioni sono le prime responsabili del processo di gestione dei rischi di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi: nel corso dell'operatività giornaliera tali strutture devono identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale, in conformità con il processo di gestione dei rischi declinato nel "Regolamento SCII"; esse devono inoltre rispettare i limiti operativi loro assegnati coerentemente con gli obiettivi di rischio e con le procedure in cui si articola il processo di gestione dei rischi.

Le Divisioni si attengono ai processi e alle procedure aziendali, verificandone l'applicazione con adeguati controlli di primo livello, diretti ad assicurare il corretto svolgimento delle operazioni, in un'ottica di piena e completa aderenza alle norme e agli standard di condotta applicabili. Le Divisioni definiscono i controlli di primo livello che considerano idonei al concreto raggiungimento degli obiettivi di controllo e procedono alla loro attuazione, coinvolgendo la Direzione Centrale Organizzazione ed il Transformation Center per gli ambiti di rispettiva competenza. I controlli di primo livello individuati dalle Divisioni sono sottoposti all'esame della Direzione Centrale Anti Financial Crime e della Direzione Centrale Compliance Governance e Controlli, che ne valutano l'idoneità al concreto raggiungimento degli obiettivi di controllo e, ove opportuno, ne richiedono il rafforzamento. Laddove le Divisioni individuino punti di criticità, direttamente o su indicazione delle competenti funzioni aziendali di controllo di secondo e terzo livello, mettono in atto le azioni necessarie alla relativa risoluzione.

Le Divisioni pongono in essere tutte le iniziative atte a favorire la diffusione di una cultura di conformità presso gli operatori, collaborando per la corretta realizzazione dei programmi di formazione definiti dalla Direzione Centrale Anti Financial Crime, in collaborazione con le competenti funzioni aziendali.

Le Divisioni rivestono un ruolo centrale ai fini della conoscenza della clientela e costituiscono, d'intesa con la Direzione Centrale Anti Financial Crime, ove ne ricorrano i presupposti in termini di efficacia ed efficienza, specifici Competence Center di Know Your Customer per lo svolgimento delle attività istruttorie per l'adeguata verifica nelle fasi di onboarding della clientela e di revisione del profilo di rischio.

Le strutture operative nell'ambito delle Divisioni, ai fini dell'adeguata verifica della clientela:

- identificano la clientela nonché i titolari effettivi e, acquisiscono e mantengono aggiornate le informazioni e la documentazione, comprese le informazioni aggiuntive in caso di rapporti con enti creditizi e finanziari, necessarie allo svolgimento degli adempimenti di adeguata verifica e all'attribuzione del profilo di rischio da associare alla clientela; qualora siano costituiti i Competence Center di Know Your Customer, forniscono ad essi tutte le informazioni disponibili sul cliente utili per espletare l'adeguata verifica della clientela e li supportano nella raccolta documentale;
- autorizzano e/o rifiutano l'apertura e il mantenimento della relazione con la clientela in fascia di rischio basso, medio basso e medio alto, tenendo in considerazione l'esito dell'istruttoria effettuata dai Competence Center qualora presenti;
- richiedono, ove necessario, l'innalzamento del profilo di rischio associato alla clientela al Competence Center che provvede ai dovuti approfondimenti e sottopone alla valutazione della Direzione Centrale Anti Financial Crime le richieste di innalzamento a rischio alto;
- prendono in autonomia la decisione in riferimento all'astensione dal rapporto o dall'esecuzione dell'operazione occasionale sulla clientela, coinvolgendo la Direzione Centrale Anti Financial Crime qualora lo ritengano opportuno;
- nell'ambito del processo di concessione effettuano attente analisi e valutazioni della clientela al fine di rilevare situazioni potenzialmente anomale sotto il profilo economico, finanziario ed organizzativo;
- comunicano alla clientela la decisione della Banca di astenersi dall'apertura di un rapporto continuativo e/o dall'esecuzione di un'operazione oppure di essere intenzionata ad estinguere un rapporto esistente.

Le strutture operative nell'ambito delle Divisioni, ai fini del monitoraggio transazionale, monitorano la relazione con il cliente e le sue operazioni al fine di individuare comportamenti anomali ed effettuare autonome valutazioni sulla propria clientela. Inoltre, per il tramite del Responsabile della struttura operativa:

- attivano, con l'ausilio della procedura dedicata, l'iter di segnalazione di operazioni sospette di primo livello ogni qual volta sia necessario;
- valutano gli inattesi intercettati dai sistemi informatici e le evidenze segnalate dalle funzioni di controllo di primo livello;
- rispondono alle comunicazioni per l'attivazione dell'iter di segnalazione di operazioni sospette, dopo aver effettuato le valutazioni del caso, al fine di confermare o meno la presenza dell'anomalia riscontrata dal secondo livello del Competence Center di Transaction Monitoring;
- riscontrano le richieste di informazioni ricevute fornendo tempestivamente le informazioni e la documentazione richiesta;
- ricevono la notifica della comunicazione di primo livello denominata "riservatissima" e attivano le valutazioni necessarie ai fini dell'eventuale avvio dell'iter di segnalazione di operazione sospetta;
- evadono le richieste di approfondimenti delle Autorità ai sensi del D. Lgs. n. 231/2007.

Le strutture operative delle Divisioni svolgono inoltre le seguenti attività:

- individuano le infrazioni alla normativa in tema di limitazioni all'uso del denaro contante e dei titoli al portatore per le quali occorre inoltrare la comunicazione al MEF e le comunicano alla Direzione Centrale Operations;
- controllano ex-ante i pagamenti e i documenti rappresentativi di merci correlati per verificare se siano conformi alle disposizioni della Direzione Centrale Anti Financial Crime in merito all'operatività con i Paesi, i settori merceologici o i soggetti sottoposti a regimi sanzionatori e/o a misure restrittive;
- controllano ex-ante i pagamenti disposti dalla/a favore della clientela per verificare che non presentino collegamenti con le liste dei soggetti considerati ad alto rischio sulla base dei criteri di profilatura della clientela adottati dal Gruppo;
- controllano, tramite la funzione che fa capo al Responsabile della struttura operativa dei controlli di linea, che le attività di monitoraggio delle operazioni e di valutazione delle infrazioni alla normativa in tema di limitazioni all'uso del denaro contante e dei titoli al portatore siano correttamente perfezionate.

Le strutture con compiti di controllo di primo livello nell'ambito delle Divisioni, in coerenza con i modelli di servizio ed organizzativi vigenti, sono responsabili di verificare il rispetto degli adempimenti in capo alle strutture operative di propria competenza, segnalando le carenze riscontrate e richiedendo gli interventi per la risoluzione delle stesse. In particolare:

- a seguito dei controlli effettuati, le strutture con compiti di controllo di primo livello trasmettono, ai sensi dell'art. 46, comma 1, lett. a), al Responsabile della struttura operativa la comunicazione c.d. "riservatissima" per attivare senza ritardo le valutazioni del caso per l'avvio dell'iter di segnalazione delle operazioni potenzialmente sospette. Di ciò informano contestualmente il Responsabile delle segnalazioni di operazioni sospette;
- l'esito delle verifiche effettuate e le eventuali carenze riscontrate sono comunicati alle strutture dell'Area di Governo Chief Compliance Officer e al Chief Audit Officer per le valutazioni di rispettiva competenza.

3.11 Altre funzioni organizzative

I principi descritti per le Divisioni trovano applicazione nei confronti delle strutture, presenti presso le Aree di Governo, con operatività con clientela e/o con controparti esterne alla Banca, per cui si applicano gli obblighi in materia di contrasto al riciclaggio, finanziamento al terrorismo e embarghi.

4. MACRO-PROCESSI PER IL CONTRASTO AI FENOMENI DI RICICLAGGIO, DI FINANZIAMENTO DEL TERRORISMO E PER LA GESTIONE DEGLI EMBARGHI

Sono stati individuati i seguenti principali macro-processi che descrivono le modalità di presidio e controllo del rischio in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi:

- definizione delle linee guida e delle regole metodologiche;
- Anti Financial Crime (AFC) Risk Assessment e risk appetite framework;
- programmazione delle attività;
- allineamento normativo;
- consulenza e clearing;
- assurance;
- diffusione della cultura in materia di antiriciclaggio, di contrasto al finanziamento del terrorismo e di gestione degli embarghi;
- interazione con le Autorità di Vigilanza e gestione degli eventi di non conformità;
- adempimenti specifici;
- flussi informativi agli Organi Societari.

4.1 *Definizione delle linee guida e delle regole metodologiche*

Il Responsabile della Direzione Centrale Anti Financial Crime, d'intesa con il Responsabile dell'Area di Governo Chief Compliance Officer, definisce le linee guida di riferimento e le regole metodologiche di presidio e di valutazione a livello di Gruppo del rischio in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi.

Le metodologie di valutazione del rischio, nelle sue componenti operativa e reputazionale, e le modalità di integrazione della valutazione di tale rischio nel Risk Appetite Framework sono definite dal Responsabile della Direzione Centrale Anti Financial Crime, d'intesa con il Responsabile dell'Area di Governo Chief Compliance Officer e con la collaborazione del Responsabile dell'Area di Governo Chief Risk Officer.

4.2 *AFC Risk Assessment e Risk Appetite Framework*

L'identificazione e la valutazione periodica del rischio e delle correlate vulnerabilità costituisce il primo momento logico del modello di gestione e risulta funzionale alla definizione dei principi di propensione al rischio e dei conseguenti limiti, da portare all'approvazione del Consiglio di Amministrazione nell'ambito del Risk Appetite Framework, e all'individuazione e programmazione degli interventi di mitigazione del rischio in materia di riciclaggio, di finanziamento del terrorismo, di violazione degli embarghi, della disciplina inerente all'operatività con soggetti attivi nel settore dei materiali di armamento¹² e di corruzione¹³.

Il Provvedimento della Banca d'Italia del 26 marzo 2019 recante disposizioni attuative in materia di organizzazione, procedure e controlli interni prevede che i destinatari svolgano una valutazione complessiva, periodicamente aggiornata, della propria esposizione al rischio di riciclaggio (c.d. autovalutazione dell'esposizione al rischio di riciclaggio) da riportare nella Relazione annuale.

¹² Con specifico riguardo all'operatività con soggetti attivi nel settore dei materiali di armamento e al RAF, si evidenzia che l'iter di valutazione rafforzato può essere esteso a operazioni riguardanti Paesi appartenenti all'Unione Europea e/o alla NATO proprio nel contesto del processo di Risk Appetite Framework.

¹³ Per la definizione di tale ambito di rischio e per il relativo quadro di riferimento si rinvia alle Linee Guida Anticorruzione di Gruppo.

Il Responsabile della Direzione Centrale Anti Financial Crime perviene con frequenza annuale - fatti salvi casi di significativa variazione dello scenario di riferimento o del perimetro operativo che richiedano valutazioni infra-annuali - alla formulazione di una valutazione dei rischi sopra richiamati (c.d. AFC Risk Assessment) per le principali entità delle singole Divisioni e del Gruppo, che sottopone al Comitato Rischi, al Comitato per il Controllo sulla Gestione e al Consiglio di Amministrazione. Tale valutazione è elaborata sulla base delle evidenze fornite dalla Direzione Centrale Anti Financial Crime (per le Banche e Società italiane del Gruppo cui si applica il modello di gestione accentrata) e dai Responsabili Antiriciclaggio (AML Officer) delle Società del Gruppo e delle Filiali Estere (cui si applica il modello di indirizzo, coordinamento e controllo).

La valutazione viene effettuata sulla base di metodologie definite dal Responsabile della Direzione Centrale Anti Financial Crime, d'intesa con il Responsabile dell'Area di Governo Chief Compliance Officer e con la collaborazione del Responsabile dell'Area di Governo Chief Risk Officer. In particolare, la metodologia di AFC Risk Assessment indaga le dimensioni del rischio inerente e delle correlate vulnerabilità, attraverso indicatori prevalentemente quantitativi integrati con valutazioni qualitative che mettono in correlazione le tipologie di rischio potenziale (ad es. livello di rischiosità della clientela, livello di rischiosità associato a Paesi non collaborativi ai fini del Regolamento Delegato (UE) 2019/758) e gli elementi di mitigazione del rischio di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi (ad es. numero di clienti per i quali è stato censito il titolare effettivo) rispetto ai dati dimensionali dell'entità in questione.

Le valutazioni del rischio a livello di Divisione derivano dall'aggregazione delle valutazioni delle entità rilevanti di ciascuna Divisione e quella di Gruppo dall'aggregazione delle valutazioni delle Divisioni. La valutazione del rischio inerente, delle vulnerabilità e del rischio residuo è espressa su una scala a quattro livelli, comune alle altre funzioni aziendali di controllo.

I modelli di valutazione del rischio in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi sono integrati nel RAF. A tal fine, nell'ambito del processo di definizione del RAF, il Responsabile della Direzione Centrale Anti Financial Crime, d'intesa con il Responsabile dell'Area di Governo Chief Compliance Officer:

- propone gli statements qualitativi relativi al rischio in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi;
- rappresenta i profili di rischio come risultanti dall'AFC Risk Assessment e propone i correlati livelli di propensione al rischio;
- declina i limiti riferiti alle perdite operative e gli altri Key Risk Indicator quantitativi rilevanti per il monitoraggio dei rischi, con focus specifico su quelli che possono costituire indicatori di violazione della normativa in ambito financial crime; in caso di superamento delle soglie fissate, ne identifica ed analizza le cause ed individua gli opportuni interventi di mitigazione, attivando, laddove necessario, i meccanismi di escalation previsti dalle Linee Guida sul RAF;
- individua, in considerazione della loro sensibilità, eventuali categorie di rischi specifici in materia di riciclaggio e di finanziamento del terrorismo per cui ritiene necessario valutare distintamente la rischiosità e prevedere la definizione di particolari orientamenti gestionali, monitoraggi operativi ed azioni di mitigazione;
- definisce le modalità di valutazione e controllo dei rischi reputazionali derivanti dalla violazione di norme imperative o di autoregolamentazione.

Le valutazioni dell'AFC Risk Assessment confluiscono anche nel Risk Assessment Integrato - predisposto nell'ambito del Comitato Coordinamento Controlli e Rischi Non Finanziari di Gruppo, sessione SCI Integrato - finalizzato a fornire una vista sintetica delle valutazioni prodotte da ciascuna funzione di controllo sul Gruppo nel suo complesso, nonché sulle principali legal entity e Divisioni, in coerenza con la metodologia in uso presso ciascuna Funzione.

4.3 Programmazione delle attività

L'identificazione e la valutazione periodica dei rischi di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi e delle correlate vulnerabilità è propedeutica alla programmazione degli interventi di gestione, da sottoporre, nel contesto delle relazioni annuali antiriciclaggio, al Consiglio di Amministrazione, previo esame da parte del Comitato Rischi e del Comitato per il Controllo sulla Gestione.

Il Responsabile della Direzione Centrale Anti Financial Crime procede annualmente alla programmazione degli interventi di gestione, fatti salvi casi di significativa variazione dello scenario di riferimento o del perimetro operativo che richiedano programmazioni infra-annuali.

La programmazione è effettuata considerando le attività che si prevede di effettuare, ripartite per macro-processi, declinate in termini di priorità, obiettivi, tempistiche e relativo assorbimento di risorse umane e finanziarie. La programmazione è supportata dall'aggiornamento delle analisi di dimensionamento svolte dalla Direzione Centrale Organizzazione, secondo logiche di priorità. Qualora dal confronto con le risorse disponibili emergano eventuali scoperture, vengono definite idonee azioni di mitigazione, basate su logiche risk-based, portate all'attenzione del Comitato Rischi, del Comitato per il Controllo sulla Gestione e del Consiglio di Amministrazione.

4.4 Allineamento normativo

Il presidio del rischio in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi si realizza, in un'ottica preventiva, in primo luogo garantendo che la normativa esterna sia costantemente monitorata e adeguatamente tradotta in linee guida, regole, processi e procedure interne. L'allineamento normativo è garantito attraverso le seguenti attività:

- l'identificazione nel continuo e l'interpretazione della normativa esterna applicabile alla Banca, tramite il monitoraggio continuativo delle fonti normative esterne e il consolidamento, in caso di evoluzione normativa, di un'interpretazione univoca e condivisa;
- la valutazione dell'impatto delle norme applicabili sui processi e le procedure aziendali e la conseguente proposizione delle modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio dei rischi.

L'attività di identificazione nel continuo della normativa esterna è svolta dalla Direzione Centrale Anti Financial Crime, con il supporto della Direzione Centrale Legale e Contenzioso – Group General Counsel ai fini dell'interpretazione della normativa.

L'attività di valutazione dell'impatto delle norme applicabili e la conseguente proposizione delle linee guida, delle regole, dei processi e delle procedure interne è presidiata dalla Direzione Centrale Anti Financial Crime, avvalendosi della collaborazione della Direzione Centrale Organizzazione e del Transformation Center e, per gli aspetti legali, della Direzione Centrale Legale e Contenzioso – Group General Counsel.

L'attività di allineamento normativo è finalizzata a definire *ex-ante* un framework funzionale al rispetto sostanziale delle norme, secondo le seguenti direttrici:

- gli indirizzi e i principi strategici per la gestione di ambiti con impatti trasversali sull'operatività del Gruppo vengono definiti in specifiche linee guida da portare all'approvazione del Consiglio di Amministrazione;
- la disciplina degli ambiti rilevanti è riportata in documenti di regole che illustrano gli aspetti metodologici, i meccanismi di funzionamento, le regole comportamentali e i vincoli a cui attenersi, anche in attuazione delle linee guida e in coerenza con gli indirizzi ivi contenuti;
- i processi, laddove standardizzati, sono supportati da procedure e strumenti informatici in grado di assistere e orientare i comportamenti del personale, così da assicurarne la correttezza;
- nei processi maggiormente sensibili le linee guida e le regole di altre strutture della Banca prevedono il coinvolgimento preventivo della Direzione Centrale Anti Financial Crime;

- i processi prevedono un sistema di controlli in grado di monitorare, nel tempo, l'efficacia dei presidi anche tenendo conto dell'evoluzione normativa e di business.

Il presidio dell'evoluzione prospettica della normativa e delle proposte di regolamentazione è agito dalla Direzione Centrale Anti Financial Crime in collaborazione con la Direzione Centrale Institutional Affairs e la struttura International Public Affairs.

4.5 Consulenza e clearing

Il presidio del rischio si realizza in un'ottica preventiva anche attraverso:

- la prestazione di consulenza ed assistenza agli Organi Societari e alle altre strutture della Banca sull'interpretazione e sull'applicazione della normativa esterna e interna;
- la valutazione preventiva della conformità alla normativa vigente, nel rispetto dei processi di Product Governance e di clearing e dei presidi previsti per le Operazioni di Maggior Rilievo, di:
 - progetti innovativi, ivi inclusi l'avvio di nuove attività e l'inserimento in nuovi mercati, individuando per questi ultimi i Paesi presso i quali qualsiasi nuovo insediamento implica un rischio ritenuto inaccettabile;
 - nuovi prodotti e servizi da avviare alla commercializzazione e/o modifiche significative di quelli esistenti;
 - fattispecie ed operazioni sensibili in relazione alle quali i processi aziendali, come disciplinati dalle linee guida e dalle regole di altre strutture della Banca, prevedano una valutazione preventiva della Direzione Centrale Anti Financial Crime, inclusa:
 - la verifica della conformità di operazioni individuate come sensibili ai fini embarghi e che coinvolgono Paesi, settori merceologici o soggetti sottoposti a regimi sanzionatori e/o a misure restrittive;
 - il parere vincolante sui presupposti antiriciclaggio in presenza dei quali si ritiene accettabile il rischio reputazionale conseguente a possibili nuovi insediamenti del Gruppo, individuando i Paesi presso i quali qualsiasi nuovo insediamento implica un rischio ritenuto inaccettabile e quelli per i quali deve essere acquisito un parere preventivo.

Le valutazioni della Direzione Centrale Anti Financial Crime sono effettuate adottando format il più possibile predefiniti che devono contenere almeno i seguenti elementi:

- oggetto della valutazione;
- contesto normativo esterno e/o interno di riferimento;
- elementi salienti della fattispecie oggetto di analisi, rilevanti ai fini delle valutazioni;
- considerazioni di sintesi da cui emergano il livello di coerenza con la lettera e lo spirito della normativa esterna e interna, gli eventuali rischi residui e le raccomandazioni formulate.

La profondità delle analisi effettuate è proporzionale al livello di complessità e novità delle fattispecie considerate e della normativa di riferimento.

4.6 Assurance

4.6.1 Il modello di assurance

Il presidio del rischio di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi si concretizza, oltre che in un'ottica preventiva, attraverso la verifica successiva dell'adeguatezza e dell'effettiva applicazione dei processi e delle procedure interne e degli adeguamenti organizzativi suggeriti per la sua prevenzione e, in genere, mediante il controllo dell'effettivo rispetto della normativa esterna e interna da parte delle strutture aziendali.

In coerenza con quanto previsto dal Regolamento del Sistema dei Controlli Interni Integrato in tema di monitoraggio e controllo dei rischi, il modello di assurance assegna:

- alle strutture operative i presidi di linea, svolti nel continuo e costantemente a valere sulle singole transazioni, e le analisi gestionali intese quali sorveglianza sistematica su fenomeni

caratterizzati da un elevato livello di anomalia che necessitano di una pronta sistemazione e/o riconduzione in ambiti di regolarità operativa e gestionale;

- alle funzioni di controllo di secondo livello il presidio della corretta applicazione del quadro di riferimento metodologico e di controllo da parte delle strutture operative tramite verifiche sia di disegno dei processi, procedure e controlli, sia dell'effettiva e corretta applicazione dei controlli previsti.

Il modello definito per la realizzazione del processo di assurance dei rischi in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi prevede che:

- in sede di definizione o revisione dei processi aziendali, anche a seguito dell'evoluzione del contesto normativo esterno, la Direzione Centrale Anti Financial Crime fissa gli obiettivi di controllo per mitigare il rischio di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi, comunicandoli alle strutture operative, nonché alle competenti strutture organizzative;
- le strutture operative, in collaborazione con la Direzione Centrale Anti Financial Crime e la Direzione Centrale Compliance Governance e Controlli, definiscono i controlli di primo livello che considerano idonei al concreto raggiungimento degli obiettivi di controllo e procedano alla loro effettuazione, coinvolgendo la Direzione Centrale Organizzazione ed il Transformation Center per gli ambiti di rispettiva competenza. I controlli di primo livello, individuati dalle Divisioni e dalle altre strutture operative, di business e di supporto sono sottoposti all'esame della Direzione Centrale Anti Financial Crime e della Direzione Centrale Compliance Governance e Controlli che ne valutano l'idoneità al concreto raggiungimento degli obiettivi di controllo e, ove opportuno, ne richiedono il rafforzamento;
- la Direzione Centrale Anti Financial Crime e la Direzione Centrale Compliance Governance e Controlli, sulla base di una valutazione del processo così definito e degli esiti dei controlli di primo livello, definiscono e svolgono i controlli di secondo livello; questi possono essere controlli a distanza di tipo andamentale sui fenomeni monitorati, controlli, anche in loco, sui processi agiti dalle strutture operative e sull'efficacia degli stessi, controlli sulla corretta esecuzione dei controlli di primo livello da parte delle strutture operative, verifiche ricorrenti o occasionali su aspetti specifici della normativa; a seconda del grado di rischio rilevato e tenuto conto dei vincoli di capacity, la periodicità dei controlli può essere continuativa, oppure periodica, su orizzonti temporali infrannuali, annuali o pluriennali, oppure *una tantum*;
- la Direzione Centrale Anti Financial Crime presidia le attività di quality assurance e svolge controlli di secondo livello di testing sugli adempimenti normativi in materia di antiriciclaggio, contrasto al finanziamento del terrorismo internazionale e di violazione degli embarghi mirati a valutare (i) la corretta applicazione dei processi di Know Your Customer, Transaction Monitoring, Financial Sanctions, conservazione e messa a disposizione di documenti, dati e informazioni, o delle loro singole fasi e (ii) la coerenza delle determinazioni assunte nei singoli processi.

4.6.2 Metodologia di svolgimento delle attività

I controlli di primo livello ed i controlli di secondo livello continuativi e periodici sono formalizzati, secondo quanto previsto dalla normativa interna aziendale, in specifiche schede di controllo che individuano la struttura responsabile, l'oggetto e le modalità di effettuazione del controllo, la relativa periodicità, i criteri di attribuzione dell'esito del controllo e le modalità della relativa rendicontazione.

I controlli di secondo livello *una tantum*, per lo più relativi a verifiche su processi e/o fenomenologie ritenute significative, sono pianificati dalla Direzione Centrale Compliance Governance e Controlli, d'intesa con la Direzione Centrale Anti Financial Crime, con periodicità di norma annuale sulla base delle risultanze dell'AFC Risk Assessment e/o di altri segnali di attenzione (ad esempio, rilievi delle Autorità di Vigilanza o delle strutture del Chief Audit Officer, richieste specifiche degli Organi Societari).

La Direzione Centrale Compliance Governance e Controlli rendiconta tali controlli alla Direzione Centrale Anti Financial Crime nonché alle strutture operative, di business e di supporto; la rendicontazione, da effettuare secondo format nei limiti del possibile predefiniti, deve contenere i seguenti elementi:

- caratteristiche dell'intervento (oggetto del controllo, contesto normativo esterno/interno di riferimento);
- dettaglio delle verifiche effettuate e relativi esiti;
- considerazioni di sintesi da cui emergano i rischi residui e le azioni di mitigazione suggerite.

Le singole unità organizzative sono responsabili della pianificazione e implementazione degli interventi correttivi; le suddette Direzioni Centrali monitorano e tracciano lo stato di avanzamento delle azioni individuate.

4.6.3 Interazioni con le altre funzioni di controllo e flussi informativi

Le modalità di collaborazione tra le funzioni aziendali di controllo e i relativi flussi informativi sono declinati nel "Regolamento SCII".

Nello svolgimento delle attività di verifica la Direzione Centrale Anti Financial Crime e la Direzione Centrale Compliance Governance e Controlli si avvalgono anche delle risultanze delle verifiche delle strutture del Chief Audit Officer che effettuano gli opportuni accertamenti sui processi e sui comportamenti, mettendo a disposizione delle strutture deputate al presidio della conformità i relativi esiti.

Inoltre, al fine di assicurare nel continuo l'efficienza e l'efficacia del sistema dei controlli a presidio dei rischi in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi sono istituiti, a livello Divisionale e ove ritenuto opportuno, specifici Tavoli a cui partecipano le funzioni di controllo di primo, secondo e terzo livello, finalizzati a:

- approfondire le evidenze emerse dalle attività di controllo, favorendo la valutazione omogenea e integrata dei rischi in questione;
- analizzare gli esiti degli accertamenti effettuati dalle Autorità di Vigilanza;
- condividere e coordinare gli interventi di remediation da attuare per il superamento delle anomalie più significative rilevate, monitorandone la realizzazione;
- pianificare le attività correlate all'implementazione e all'aggiornamento del sistema dei controlli in termini di predisposizione e revisione della relativa normativa interna, individuazione degli eventuali adeguamenti procedurali e definizione dei conseguenti flussi informativi con l'obiettivo di impostare le attività di controllo in modo coerente e integrato.

La Direzione Centrale Anti Financial Crime e la Direzione Centrale Compliance Governance e Controlli hanno accesso a tutte le attività della Banca nonché a qualsiasi informazione rilevante per lo svolgimento dei propri compiti, anche attraverso il colloquio diretto con il personale. A tal fine:

- sono destinatarie e mittenti dei flussi informativi riportati nel "Regolamento SCII";
- le altre strutture aziendali devono comunicare loro, in modo tempestivo e completo, ogni eventuale fatto rilevante ai fini del presidio dei rischi in questione;
- possono chiedere e ricevere dalle altre funzioni aziendali tutte le eventuali ulteriori informazioni rilevanti per l'assolvimento dei propri compiti.

4.6.4 Processo di follow up

Lo sviluppo delle azioni di mitigazione del rischio attivate per la risoluzione delle criticità emerse dai controlli di assurance ed il rispetto delle relative scadenze sono oggetto di follow up nel continuo da parte della Direzione Centrale Anti Financial Crime, attraverso specifici meccanismi definiti in funzione della rilevanza della criticità e supportati da adeguati strumenti di monitoraggio dello stato delle singole attività e dell'evoluzione dei gap identificati, al fine di provvedere, a fronte di ritardi significativi, all'avvio delle necessarie iniziative di escalation.

4.7 Diffusione della cultura in materia di antiriciclaggio, contrasto al finanziamento del terrorismo ed embarghi

La diffusione, a tutti i livelli aziendali, di una cultura improntata ai principi di onestà, correttezza e rispetto dello spirito e della lettera delle norme è un presupposto fondamentale per il presidio del rischio. Un'efficace applicazione della normativa antiriciclaggio, di contrasto al finanziamento del terrorismo e di gestione degli embarghi non può inoltre prescindere dalla piena consapevolezza delle finalità e dei principi che ne sorreggono l'impianto.

La Direzione Centrale Anti Financial Crime collabora con la Direzione Centrale Politiche di Sviluppo e Learning Academy, la Direzione Centrale People Management & HR Transformation, le funzioni HR delle diverse Divisioni e la Comunicazione Interna per l'istituzione di canali di comunicazione e strumenti di formazione efficaci, identificando i fabbisogni formativi relativi alle materie di competenza e predisponendo i contenuti delle iniziative di formazione per tutte le risorse della Banca, nell'ottica di garantire che il personale, con particolare attenzione agli addetti alla vendita dei prodotti e ai responsabili delle strutture di business, abbia un'adeguata conoscenza della normativa di riferimento, degli obblighi e delle connesse responsabilità, delle conseguenze derivanti dal mancato adempimento di tali obblighi e sia in grado di utilizzare consapevolmente strumenti e procedure di ausilio nell'esecuzione degli adempimenti stabiliti dalla normativa.

La Direzione Centrale Anti Financial Crime, con la collaborazione della Direzione Centrale Politiche di Sviluppo e Learning Academy, della Direzione Centrale People Management & HR Transformation e delle funzioni HR delle diverse Divisioni monitora l'evoluzione dei programmi formativi, verificandone la fruizione¹⁴ e l'efficacia, e fornisce adeguata evidenza agli Organi Societari, anche per la tempestiva individuazione degli interventi correttivi eventualmente necessari.

Accanto alle attività formative tradizionali, la Direzione Centrale Anti Financial Crime, sotto l'egida del Comitato Coordinamento Controlli e rischi Non Finanziari di Gruppo e in collaborazione con la Direzione Centrale Politiche di Sviluppo e Learning Academy, organizza e partecipa a specifiche iniziative finalizzate a diffondere la cultura del rischio e ad ampliare il livello di consapevolezza dell'approccio al rischio richiesto, tra cui in particolare:

- sessioni di induction per gli Organi Societari e workshop per il top management su temi particolarmente delicati o di attualità;
- interventi di sensibilizzazione delle strutture operative, di business e di supporto su aspetti specifici di rischio tratti dall'ordinaria operatività;
- attività diagnostiche finalizzate ad apprezzare il grado di diffusione della cultura del rischio a tutti i livelli aziendali, in termini di congruenza delle percezioni e dei comportamenti agiti rispetto agli indirizzi e orientamenti desiderati.

Sono inoltre previsti specifici programmi di formazione per il personale della Direzione Centrale Anti Financial Crime, affinché quest'ultimo sia costantemente aggiornato sull'evoluzione dei rischi in materia, nonché specifiche sessioni di induction per gli AML Officer delle Società del Gruppo e Filiali Estere sui rischi in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi.

4.8 Interazione con le Autorità di Vigilanza e gestione degli eventi di non conformità

Un momento di particolare rilevanza nel presidio del rischio è costituito dalla gestione delle relazioni con le Autorità di Vigilanza e dalla gestione degli eventi di non conformità. La Direzione Centrale Anti Financial Crime provvede, per gli ambiti di competenza, a gestire:

¹⁴ Mediante gli strumenti messi a disposizione dalla Direzione Centrale Politiche di Sviluppo e Learning Academy.

- le relazioni con le Autorità di Vigilanza, coordinando le attività necessarie per il riscontro alle richieste delle Autorità medesime;
- gli eventi di non conformità, fornendo assistenza e collaborazione all'unità interessata al fine di assicurare l'individuazione e l'implementazione delle azioni da intraprendere per colmare gli eventuali gap organizzativi e/o procedurali.

I processi di interazione comprendono inoltre l'invio di reportistica specifica alle Autorità di Vigilanza, secondo i requisiti definiti dalla normativa in tema di antiriciclaggio, di contrasto al fenomeno del terrorismo e di gestione degli embarghi. Tale reportistica include:

- l'invio all'UIF dei dati aggregati concernenti le registrazioni nell'archivio di conservazione;
- l'invio all'UIF delle segnalazioni di operazioni sospette;
- l'invio all'UIF ed al Nucleo Speciale della Guardia di Finanza delle comunicazioni inerenti al congelamento di fondi e risorse economiche riconducibili ai soggetti designati destinatari di misure restrittive nell'ambito della normativa sugli embarghi e sul contrasto al finanziamento del terrorismo;
- l'invio all'UIF delle periodiche comunicazioni oggettive¹⁵ concernenti operazioni a rischio, in conformità alle disposizioni di attuazione emanate dall'UIF.

4.9 Adempimenti specifici

4.9.1 Adeguata verifica della clientela

Gli adempimenti di adeguata verifica della clientela sono commisurati alla valutazione dell'effettivo grado di rischio di riciclaggio e di finanziamento del terrorismo associato al cliente. La valutazione del rischio di riciclaggio e di finanziamento del terrorismo è effettuata in considerazione delle caratteristiche del cliente, della sua condotta e delle specificità del rapporto continuativo o dell'operazione che il medesimo vuole porre in essere, considerando i criteri indicati dalla normativa di riferimento.

Sulla base del livello di rischio associato al cliente, si applica la seguente diversa gradazione della modalità di conduzione delle attività di adeguata verifica:

- obblighi ordinari;
- obblighi semplificati;
- obblighi rafforzati.

Gli adempimenti di adeguata verifica devono essere attuati (i) in relazione ai rapporti ed alle operazioni che rientrano nell'attività istituzionale, (ii) in tutti i casi in cui vi è sospetto di riciclaggio o di finanziamento del terrorismo, indipendentemente da qualsiasi deroga, esenzione o soglia applicabile e (iii) quando vi sono dubbi sulla veridicità o sull'adeguatezza dei dati precedentemente ottenuti.

L'impossibilità di rispettare gli adempimenti previsti in tema di adeguata verifica della clientela comporta l'obbligo di astenersi dall'instaurare il rapporto continuativo o dall'eseguire un'operazione oppure di valutare se procedere all'interruzione di un rapporto già in essere. In questi casi occorre inoltre valutare se inviare una segnalazione di operazione sospetta.

Gli obblighi di adeguata verifica della clientela si attuano attraverso:

- l'identificazione della clientela, dell'eventuale esecutore e dei titolari effettivi e la verifica dell'identità di tali soggetti: l'identificazione avviene tramite l'acquisizione dei documenti identificativi, oppure di attestazioni di adeguata verifica rilasciate da altri intermediari e di eventuali informazioni aggiuntive necessarie a determinare il profilo di rischio da associare al

¹⁵ Con riferimento alle Società Estere del Gruppo, solo se previsto dalla normativa nazionale di riferimento.

cliente; la verifica dell'identità dei soggetti citati avviene sulla base di documenti, dati ed informazioni ottenuti da una fonte affidabile ed indipendente;

- la profilatura del cliente in base al rischio di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi: la profilatura avviene tramite l'assegnazione di un punteggio - elaborato sulla base dei dati e delle informazioni acquisite in sede di accensione del rapporto e di monitoraggio delle attività - e la conseguente classificazione dei clienti in quattro fasce a seconda che il rischio sia considerato alto, medio alto, medio basso o basso¹⁶; nel caso di clienti a rischio alto o medio alto si applicano gli obblighi di adeguata verifica rafforzata. La profilatura è assoggettata ad un processo di armonizzazione a livello di Gruppo in base al quale ciascuna Società del Gruppo assume, per uno stesso cliente, il profilo di rischio più elevato tra quelli assegnati dalle altre Società del Gruppo;
- l'autorizzazione all'apertura di un nuovo rapporto, all'esecuzione di un'operazione occasionale o al mantenimento di un rapporto già in essere tenendo conto del profilo di rischio associato al cliente: per i clienti a rischio alto o medio alto per cui si applicano gli obblighi di adeguata verifica rafforzata, l'autorizzazione viene rilasciata: (i) per i clienti a rischio alto dalla Direzione Centrale Anti Financial Crime, fatte salve eventuali sub-deleghe attribuite dal Responsabile di tale Direzione ad altre strutture della Banca sulla base di criteri oggettivi e predeterminati; (ii) per i clienti a rischio medio alto dalla struttura operativa. È fatta eccezione per le Persone Politicamente Esposte, i rapporti e le operazioni che coinvolgono Paesi terzi ad alto rischio ed i rapporti di corrispondenza con enti creditizi o finanziari corrispondenti di un Paese extra SEE, per i quali l'autorizzazione viene rilasciata da un alto dirigente sulla base di specifiche deleghe rilasciate dal Consigliere Delegato e CEO;
- l'autorizzazione o meno a procedere, rilasciata dalla Direzione Centrale Anti Financial Crime, per la clientela che, in fase di censimento, apertura di un rapporto o aggiornamento anagrafico, presenti un riscontro positivo con le Sanction List o con le liste antiterrorismo anche a seguito delle verifiche effettuate dalle competenti funzioni della Direzione Centrale Operations;
- l'aggiornamento periodico delle informazioni relative all'adeguata verifica e la revisione periodica del profilo di rischio per i clienti con grado di rischio alto o medio alto, rispettivamente ogni 18 e 24 mesi¹⁷, eccezion fatta per (i) le Persone Politicamente Esposte, per cui l'aggiornamento dei dati e la rivalutazione avviene ogni 18 mesi; (ii) per la clientela Financial Institutions, per cui l'aggiornamento dei dati e la rivalutazione avviene ogni 12 mesi per i clienti in fascia di rischio alto e medio alto, ogni 24 mesi per i clienti in fascia di rischio medio basso e ogni 36 mesi per i clienti in fascia di rischio basso;
- l'aggiornamento delle informazioni relative all'adeguata verifica e la rivalutazione della relazione al verificarsi di determinati eventi (c.d. "event driven review"), quali (i) l'acquisizione dello status di Persona Politicamente Esposta; (ii) la segnalazione di operazione sospetta; (iii) la notifica di un accertamento di natura penale; (iv) la variazione di un titolare effettivo; (v) la modifica della residenza del titolare effettivo qualora la nuova risulti in un Paese ad alto rischio.

Lo svolgimento delle attività istruttorie per l'adeguata verifica, nelle fasi di onboarding della clientela e di revisione del profilo di rischio, avviene, ove ne ricorrano i presupposti in termini di efficacia ed efficienza, tramite il Competence Center di Know Your Customer.

4.9.1.1 Obblighi ordinari di adeguata verifica

Per i clienti che non presentano un elevato profilo di rischio di riciclaggio e di finanziamento del terrorismo, classificati nelle fasce di rischio basso o medio basso, sussistono obblighi ordinari di adeguata verifica, che consistono nell'identificazione del cliente, dell'eventuale esecutore e del

¹⁶ La nomenclatura delle fasce di rischio nei diversi applicativi utilizzati per la profilatura della clientela sarà gradualmente allineata a quanto previsto dalle presenti Linee Guida; nelle more la riconduzione alle fasce di rischio adottate è riportata nelle regole metodologiche di riferimento.

¹⁷ Per la clientela delle Filiali Estere le periodicità di aggiornamento e revisione sono: 12 mesi per i clienti in fascia di rischio alto, 24 mesi per i clienti in fascia di rischio medio alto e 36 mesi per i clienti in fascia di rischio medio basso e basso ad eccezione delle Filiali di Shanghai e Dubai per le quali la periodicità di aggiornamento è di 24 mesi. .

titolare effettivo, nella verifica dell'identità dei soggetti citati sulla base di documenti, dati ed informazioni ottenuti da una fonte affidabile ed indipendente, nell'acquisizione e valutazione delle informazioni sullo scopo e sulla natura del rapporto continuativo o dell'operazione occasionale, nella verifica dell'eventuale presenza di notizie negative sul cliente, oltre che nel controllo costante nel corso del rapporto continuativo.

4.9.1.2 Operatività a distanza

L'operatività a distanza, intendendosi per tale l'operatività svolta senza la compresenza fisica presso la Banca del cliente, dei dipendenti o di altro personale incaricato dalla Banca, richiede particolari cautele nello svolgimento dell'adeguata verifica, anche in considerazione del rischio di frodi connesse al furto di identità.

In tal senso, la Banca procede con:

- l'acquisizione dei dati identificativi del cliente e dell'eventuale esecutore ed il loro riscontro su una copia – ottenuta tramite fax, posta, in formato elettronico o con modalità analoghe – di un valido documento di identità ai sensi della normativa vigente; e
- l'effettuazione di riscontri ulteriori rispetto a quelli ordinari relativi al processo di identificazione della clientela, secondo un approccio basato sul rischio, attraverso una o più delle seguenti misure: (i) contatto telefonico su utenza fissa (welcome call), (ii) invio di comunicazioni a un domicilio fisico con ricevuta di ritorno, (iii) bonifico effettuato dal cliente attraverso un intermediario bancario e finanziario con sede in Italia o in un Paese dell'Unione Europea, (iv) richiesta di invio di documentazione controfirmata, (v) verifica su residenza, domicilio, attività svolta, tramite richieste di informazioni ai competenti uffici ovvero mediante incontri in loco, effettuati avvalendosi di personale proprio o di terzi, (vi) meccanismi di riscontro basati su soluzioni che prevedono sicure forme di riconoscimento biometrico.

In alternativa, la mitigazione del rischio avviene effettuando l'identificazione del cliente persona fisica da remoto secondo procedure rafforzate in coerenza con il Provvedimento della Banca d'Italia del 30 luglio 2019 recante le disposizioni attuative in materia di adeguata verifica della clientela.

4.9.1.3 Obblighi semplificati di adeguata verifica

In presenza di un ridotto rischio di riciclaggio o di finanziamento del terrorismo, gli obblighi di adeguata verifica possono essere assolti in maniera semplificata, riducendo l'estensione e la frequenza degli adempimenti ordinari previsti. Rientrano in tale tipologia, salvo diversa determinazione assunta ad hoc in relazione allo specifico cliente in esame, le seguenti categorie di clientela:

- intermediari bancari e finanziari di cui all'art. 3, comma 2, del D. Lgs. n. 231/2007, esclusi gli agenti di cambio, gli intermediari assicurativi che operano nei rami vita, le società fiduciarie iscritte nell'albo ex art. 106 TUB, i consulenti finanziari e le società di consulenza finanziaria di cui agli artt. 18-bis e 18-ter del TUF;
- società quotate su mercati regolamentari e sottoposte ad obblighi di comunicazione che includano quelli di assicurare un'adeguata trasparenza della titolarità effettiva;
- pubbliche amministrazioni, istituzioni od organismi che svolgono funzioni pubbliche conformemente al diritto dell'Unione Europea;
- intermediari bancari e finanziari comunitari o con sede in un Paese extra SEE con un efficace regime di contrasto del riciclaggio e del finanziamento del terrorismo individuato sulla base degli indicatori usati per determinare tali rischi.

L'applicazione dell'adeguata verifica semplificata comporta in ogni caso:

- la raccolta delle informazioni necessarie per identificare il cliente, l'eventuale esecutore ed il titolare effettivo e la verifica della relativa identità;
- la ricostruzione, con riferimento alla titolarità effettiva, della catena di controllo basandosi o sulla dichiarazione del cliente o su fonti esterne attendibili;

- l'acquisizione delle informazioni sullo scopo/natura del rapporto, utilizzando anche delle presunzioni nella loro individuazione laddove il prodotto sia destinato ad uno specifico utilizzo;
- la raccolta di ogni altra informazione necessaria alla profilatura del cliente ricorrendo anche ad informazioni desumibili da fonti pubbliche (siti istituzionali delle Autorità di Vigilanza, siti degli intermediari interessati, bilanci ove disponibili, info provider esterni);
- l'esercizio di un controllo costante nel corso del rapporto continuativo;
- la conservazione dei dati e delle informazioni relative ai rapporti ed all'operatività secondo modalità predefinite.

L'assolvimento in modo semplificato degli obblighi di adeguata verifica è subordinato alla verifica nel continuo del permanere dei relativi presupposti.

Le misure di adeguata verifica semplificata non trovano applicazione quando:

- sussistono dubbi, incertezze o incongruenze in relazione ai dati identificativi ed alle informazioni acquisite in sede di identificazione del cliente, dell'eventuale esecutore ovvero del titolare effettivo;
- vengono meno le condizioni per l'applicazione delle misure semplificate, in base agli indici di rischio previsti dalla normativa applicabile in materia;
- le attività di monitoraggio sulla complessiva operatività del cliente e le informazioni acquisite nel corso del rapporto inducono ad escludere la presenza di una fattispecie a basso rischio di riciclaggio e di finanziamento del terrorismo;
- sussiste comunque il sospetto di riciclaggio o di finanziamento del terrorismo.

4.9.1.4 Obblighi rafforzati di adeguata verifica

Per i clienti classificati a rischio elevato, collocati nelle fasce di rischio alto o medio alto, si applicano misure rafforzate di adeguata verifica, la cui profondità è dipendente dalla classificazione del cliente nelle due diverse fasce di rischio. Vengono sempre considerati a rischio elevato:

- particolari tipologie di rapporti ed operazioni:
 - i rapporti e le operazioni occasionali che coinvolgono: (i) Paesi terzi ad alto rischio così come definiti nel Regolamento UE 1675/2016 e successivi aggiornamenti, (ii) Paesi sottoposti a sanzioni sotto il profilo embarghi, (iii) Paesi che presentano criticità sotto il profilo della cooperazione in ambito fiscale, (iv) Paesi presenti negli specifici elenchi del GAFI "High Risk Jurisdictions subject to a Call for Action" e "Jurisdictions under Increased Monitoring";
 - i conti di corrispondenza, che comportano l'esecuzione di pagamenti, e rapporti assimilabili con enti creditizi e finanziari con sede in un Paese extra SEE;
 - operazioni con banconote di grosso taglio;
 - operazioni con importi insolitamente elevati o rispetto alle quali sussistono dubbi circa la loro finalità;
 - operazioni di versamento denaro/valori provenienti da altri Stati;
- particolari tipologie di clientela:
 - Persone Politicamente Esposte;
 - altre tipologie di clientela considerate a rischio elevato quali: (i) soggetti che esercitano in via esclusiva l'attività di "Compro Oro", (ii) trust e società fiduciarie non facenti parte del Gruppo Intesa Sanpaolo (indipendentemente dal fatto che siano iscritte all'Albo previsto dall'art. 106 del TUB) e loro partecipate, (iii) Money Transfer italiani ed esteri e loro agenti che effettuano rimesse di denaro, (iv) clientela interessata dall'erogazione di fondi pubblici/aggiudicataria di appalti pubblici, (v) operatori in giochi e scommesse, (vi) clientela aderente al Sistema di Protezione per Richiedenti Asilo e Rifugiati (SPRAR), (vii) intermediari finanziari o creditizi esteri non soggetti agli obblighi di autorizzazione all'esercizio dell'attività da parte dell'Autorità di Vigilanza del Paese di insediamento, (viii) prestatori di servizi relativi all'utilizzo di valuta virtuale (Virtual Asset Services Provider – VASP), (ix) società che hanno emesso azioni al portatore, (x) soggetti attivi nel settore dei materiali di armamento.

Le misure di adeguata verifica rafforzata consistono:

- nella raccolta di maggiori informazioni relative:
 - al cliente, all'eventuale esecutore ed al titolare effettivo o all'assetto proprietario e di controllo per verificare i dati e le informazioni minimali, compresa l'acquisizione e la valutazione delle informazioni di natura reputazionale, sul cliente e sul titolare effettivo;
 - al rapporto per comprenderne appieno la natura e lo scopo, acquisendo informazioni sulla natura dell'attività svolta dal cliente e/o dal titolare effettivo, la destinazione dei fondi, le ragioni per cui il cliente richiede un determinato prodotto/servizio;
- nella maggior frequenza ed intensità delle verifiche svolte nell'ambito del controllo costante del rapporto continuativo, da espletarsi mediante l'aggiornamento delle informazioni e della profilatura, l'esame delle operazioni significative o anomale e della movimentazione complessiva, anche per tipologie di importi e di operazioni non considerate dalle procedure automatiche di monitoraggio o di aggregazione;
- nella verifica dell'origine del patrimonio e dei fondi del cliente, impiegati nel rapporto continuativo;
- nell'attivazione di uno specifico iter autorizzativo, più rigoroso rispetto a quello ordinariamente previsto, in fase di accensione del rapporto o di compimento di operazioni occasionali o di valutazioni circa il mantenimento del rapporto. In particolare, per i rapporti e le operazioni occasionali con clienti Persone Politicamente Esposte, in presenza di rapporti o operazioni che coinvolgono Paesi terzi ad alto rischio, nonché per i rapporti di corrispondenza con enti creditizi o finanziari aventi sede in Paesi extra SEE, è prevista una specifica autorizzazione da parte di un alto dirigente sulla base di specifiche deleghe rilasciate dal Consigliere Delegato e CEO.

4.9.1.5 Esecuzione degli obblighi di adeguata verifica da parte di terzi

La Banca può avvalersi, a determinate condizioni, dell'adeguata verifica svolta da parte di un soggetto terzo, che attesti il corretto adempimento degli obblighi antiriciclaggio per le varie attività effettuate. Qualora il soggetto terzo sia:

- un intermediario bancario o finanziario (o altre situazioni equiparate dalla normativa), esso può svolgere tutte le fasi dell'adeguata verifica ad eccezione del controllo costante dell'operatività;
- un mediatore creditizio o un agente in attività finanziaria (o altre situazioni equiparate dalla normativa), esso può procedere unicamente all'identificazione del cliente, dell'esecutore e del titolare effettivo, inclusa l'acquisizione di copia dei documenti identificativi.

È possibile far affidamento sull'identificazione e sulle risultanze delle altre fasi di adeguata verifica già svolte dal soggetto terzo nei casi in cui:

- per il tipo di prodotto/servizio offerto, per le modalità dell'offerta o per effettive difficoltà pratiche, non sia possibile l'identificazione di persona, fuori sede o a distanza a cura dei dipendenti o dei consulenti finanziari abilitati dalla Banca, o di collaboratori o soggetti esterni di cui la Banca si avvale;
- si ritenga di dover esperire ulteriori verifiche sul cliente già identificato, attingendo alle informazioni in possesso del soggetto terzo.

In tali circostanze, il soggetto terzo rilascia alla Banca un'idonea attestazione dell'assolvimento degli obblighi di identificazione o adeguata verifica del cliente, per il quale ha provveduto ad adempierli in proprio, in presenza del cliente o a distanza, in relazione a un rapporto continuativo o all'esecuzione di un'operazione occasionale.

In nessun caso gli obblighi di adeguata verifica possono essere demandati dalla Banca a banche di comodo o intermediari insediati in Paesi terzi ad alto rischio, così come definiti nel Regolamento UE 1675/2016 e successivi aggiornamenti, o le cui legislazioni locali impediscano adeguati presidi dei rischi di riciclaggio o di finanziamento del terrorismo e, in particolare, la condivisione nell'ambito del proprio gruppo dei dati e delle informazioni relative alla propria clientela.

4.9.2 Conservazione e messa a disposizione dei documenti, dei dati e delle informazioni

Per l'assolvimento degli obblighi di conservazione vengono conservati:

- la copia dei documenti acquisiti in occasione dell'adeguata verifica della clientela;
- le scritture e le registrazioni delle operazioni e dei rapporti continuativi, consistenti nei documenti originali o nelle copie aventi analoga efficacia probatoria nei procedimenti giudiziari.

I documenti, i dati e le informazioni acquisiti sono conservati per un periodo di dieci anni dalla cessazione del rapporto continuativo o della prestazione professionale o dall'esecuzione dell'operazione occasionale.

Per garantire la ricostruibilità dell'operatività della clientela e per agevolare lo svolgimento delle funzioni di controllo delle autorità competenti, i dati e le informazioni vengono resi disponibili alle medesime autorità, secondo gli standard previsti dalle vigenti disposizioni in materia e senza applicare alcuna esenzione, mediante l'Archivio Unico Informatico (AUI); tale archivio viene gestito dalla Direzione Centrale Anti Financial Crime e dalla Direzione Centrale Sistemi Informativi, ciascuna per i profili di competenza e per gli ambiti di responsabilità, nell'ottica di garantire la chiarezza e la completezza delle informazioni, la loro conservazione e la facilità di consultazione. Sulla base di tale archivio vengono inoltre determinati i dati aggregati concernenti l'operatività della Banca da trasmettere all'UIF, a cura della Direzione Centrale Anti Financial Crime.

I dati e le informazioni sono resi disponibili alle autorità per i dieci anni successivi alla chiusura del rapporto o al compimento dell'operazione.

4.9.3 Monitoraggio delle transazioni

Gli obblighi di monitoraggio transazionale si attuano attraverso il controllo costante dei rapporti continuativi al fine di verificare la coerenza dell'operatività con lo scopo del rapporto dichiarato dal cliente stesso, intercettando eventuali operazioni "inattese", anomale o non coerenti rispetto al profilo economico e finanziario del cliente o eventuali notizie di eventi significativi che lo riguardino.

Per garantire il controllo delle transazioni/operazioni svolte dalla clientela i principali processi sono:

- controllo ex-ante, a cura delle strutture operative che eseguono le transazioni, allo scopo di individuare, bloccare e segnalare quelle che evidenzino sospetti di riciclaggio, finanziamento del terrorismo, violazioni della normativa in tema di embarghi, nonché in tema di limitazioni all'uso del contante e dei titoli al portatore. Le strutture operative possono avvalersi del supporto della struttura di consulenza della Direzione Centrale Anti Financial Crime per valutare se sussistano i presupposti per astenersi dall'effettuare un'operazione. Nel caso in cui tali presupposti si ritengano sussistenti, le strutture operative comunicano con il Responsabile delle segnalazioni di operazioni sospette perché quest'ultimo valuti se astenersi dall'esecuzione dell'operazione e chiedere all'UIF il provvedimento di sospensione nei casi di rischio evidente;
- controllo ex-ante dei pagamenti e dei documenti rappresentativi di merci mediante confronto con le Sanction List e/o le liste antiterrorismo o liste interne al Gruppo e la verifica dei riscontri prodotti dalle procedure di controllo. Tali verifiche coinvolgono in prima istanza la Direzione Centrale Operations e le strutture operative che eseguono le transazioni, le quali richiedono alla Direzione Centrale Anti Financial Crime ove necessario l'autorizzazione al proseguimento delle operazioni;
- monitoraggio ex-post a cura del Competence Center di Transaction Monitoring delle transazioni della clientela e dell'operatività di "tramitazione" o "pass through" con valutazione delle transazioni potenzialmente anomale. Il Competence Center di Transaction Monitoring effettua le analisi del caso tramite una struttura a due livelli, ove la Direzione Operations è responsabile delle attività di analisi delle evidenze prodotte dai sistemi automatici e la Direzione Centrale Anti Financial Crime delle ulteriori analisi delle transazioni non archiviate dalla Direzione Operations in quanto falsi positivi. Le transazioni valutate dalla Direzione Centrale Anti Financial Crime come

meritevoli di considerazione sono sottoposte al Responsabile della struttura operativa competente al fine dell'avvio dell'iter di segnalazione di operazione sospetta.

Inoltre, per ridurre il rischio di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi ed i connessi rischi reputazionali, legali ed operativi, tenuto conto delle specifiche norme al riguardo, il Gruppo Intesa Sanpaolo:

- non effettua i cosiddetti “cover payments”, intendendosi con tale definizione i pagamenti nei quali le informazioni relative a ordinante e beneficiario della transazione viaggiano tipicamente in un messaggio diverso da quello relativo alla movimentazione dei fondi e che non transita necessariamente in un sistema di pagamento;
- non opera con i cosiddetti “payable-through accounts” o “conti di passaggio”, intendendosi con tale definizione i rapporti bancari di corrispondenza transfrontalieri intrattenuti tra intermediari finanziari con diretto utilizzo da parte dei clienti dell'intermediario finanziario (ad. esempio, mediante traenza di assegni sul conto di corrispondenza).

4.9.3.1 Monitoraggio dei trasferimenti di fondi

In ottemperanza alle previsioni del Regolamento (UE) 847/2015, che individua le informazioni sull'ordinante e sul beneficiario che devono accompagnare i trasferimenti di fondi, vengono attuati specifici controlli al fine di verificare che i trasferimenti di fondi siano corredati delle informazioni richieste. La procedura adottata prevede una combinazione di controlli ex post ed ex ante. Tali verifiche coinvolgono in prima istanza la Direzione Centrale Operations e le strutture degli AML Officer¹⁸.

4.9.4 Segnalazione delle Operazioni Sospette

Al fine di garantire l'assolvimento degli obblighi in tema di segnalazione delle operazioni ritenute sospette, la procedura di segnalazione, in coerenza con le previsioni normative, è distinta in due fasi¹⁹:

- segnalazione di primo livello, il cui obbligo fa capo ai Responsabili delle strutture operative aziendali che, rilevate le operazioni della specie, sono tenuti a segnalarle senza ritardo al Responsabile delle segnalazioni di operazioni sospette; le segnalazioni in oggetto possono essere originate sia dalle evidenze provenienti dal Competence Center di Transaction Monitoring sia dall'autonoma attività di monitoraggio svolta dai Responsabili delle strutture operative;
- segnalazione di secondo livello, il cui obbligo fa capo alla struttura aziendale individuata all'interno della Direzione Centrale Anti Financial Crime che esamina le segnalazioni ricevute e, qualora le ritenga fondate, le trasmette all'UIF. Nel predetto esame rientrano le segnalazioni di operazioni ritenute sospette in materia di riciclaggio, di finanziamento del terrorismo o di finanziamento di programmi di proliferazione di armi di distruzione di massa, pervenute dalle strutture operative.

La segnalazione di primo livello dei Responsabili delle strutture operative aziendali può essere originata anche dal recepimento da parte di questi ultimi delle comunicazioni denominate “riservatissime” trasmesse ad esito delle attività di controllo svolte dalle strutture del Chief Audit Officer e dell'Area di Governo Chief Compliance Officer, nonché dalle strutture con compiti di controllo di primo livello presso le Divisioni.

¹⁸ Alla data di pubblicazione delle presenti Linee Guida i controlli ex ante sono agiti sui trasferimenti transfrontalieri delle Filiali estere di London, Dubai, Hong Kong, Shanghai, Singapore, Tokyo, Abu Dhabi, Amsterdam, Francoforte, Parigi, Madrid e Varsavia e saranno oggetto di progressiva estensione.

¹⁹ Con riferimento alle Società Estere del Gruppo solo se previsto dalla normativa nazionale di riferimento.

I dati e le informazioni relative alle segnalazioni di operazioni sospette sono condivisi a livello di Gruppo, salvo il rispetto dei limiti imposti dagli ordinamenti ove hanno sede le Società e le Filiali Estere.

4.9.5 Gestione del rischio in ambito extra SEE

In ottemperanza alle previsioni contenute nel Regolamento Delegato (UE) 2019/758, che disciplina l'azione minima ed il tipo di misure supplementari da adottare per mitigare il rischio di riciclaggio e di finanziamento del terrorismo nei Paesi extra SEE, la Direzione Centrale Anti Financial Crime, nell'ambito dell'adozione di metodologie di Gruppo, si adopera affinché le procedure presso le succursali e filiazioni del Gruppo con sede in tali Paesi terzi siano allineate agli standard di Gruppo e consentano la condivisione nell'ambito dello stesso delle informazioni rilevanti sulla clientela, incluse le informazioni relative ad operazioni sospette, salvo il rispetto dei limiti imposti dall'ordinamento locale.

Ove l'ordinamento del Paese extra SEE non consenta alle succursali e filiazioni del Gruppo ivi stabilite di adeguarsi agli standard di Gruppo ovvero di condividere nell'ambito dello stesso le informazioni rilevanti sulla clientela, la Direzione Centrale Anti Financial Crime, in coerenza con le previsioni del Regolamento Delegato (UE) 2019/758, ne dà comunicazione alla Banca d'Italia e dispone l'applicazione di misure supplementari, secondo un approccio basato sul rischio.

4.10 Flussi informativi agli Organi Societari

I processi di comunicazione nei confronti degli Organi Societari prevedono:

- programmazione delle attività presentata, con cadenza di norma annuale, per approvazione al Consiglio di Amministrazione, previo esame del Comitato Rischi e del Comitato per il Controllo sulla Gestione;
- relazione semestrale inviata al Consiglio di Amministrazione, al Comitato Rischi e al Comitato per il Controllo sulla Gestione sulle attività di verifica svolte, sulle iniziative intraprese, sulle disfunzioni accertate e sulle relative azioni correttive da intraprendere nonché sull'attività formativa del personale;
- informativa sulle infrazioni gravi o ripetute o sistematiche o plurime ai sensi dell'art. 46, comma 1, lett. b) e delle infrazioni dell'art. 51, comma 1, del D. Lgs. n. 231/2007, inviata al Comitato per il Controllo sulla Gestione con cadenza semestrale o alla prima riunione utile in caso di infrazioni di particolare gravità; solo successivamente è prevista una comunicazione all'Autorità di Vigilanza o al MEF;
- specifiche informative su tematiche di particolare rilevanza.

5. INDIRIZZO E COORDINAMENTO DEL GRUPPO

Il Gruppo, in considerazione della sua articolazione operativa e territoriale, intende adottare un approccio unitario in materia di antiriciclaggio, di contrasto al finanziamento del terrorismo e di gestione degli embarghi, con linee guida, regole, processi, controlli e strumenti informatici ragionevolmente omogenei a livello di Gruppo. A tal fine le Società del Gruppo sono tenute a recepire le presenti Linee Guida, adeguandole al proprio contesto societario e, nel caso di Società Estere, alle specificità delle normative locali, sottoponendole all'approvazione dell'Organo con funzioni di supervisione strategica.

Le decisioni strategiche a livello di Gruppo in materia di gestione dei rischi di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi sono rimesse agli Organi Societari della Capogruppo. Gli Organi Societari delle Società del Gruppo devono essere consapevoli delle scelte effettuate dagli Organi Societari della Capogruppo e sono responsabili, ciascuno secondo le proprie competenze, dell'attuazione delle strategie e politiche di gestione dei rischi di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi in coerenza con la propria realtà aziendale. In tale ottica, la Capogruppo coinvolge e rende partecipi, tramite il Responsabile Antiriciclaggio di Gruppo, gli Organi Societari delle Società del Gruppo circa le scelte adottate in materia di politiche, processi e procedure di gestione dei rischi di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi.

Nell'ambito del Gruppo Intesa Sanpaolo gli specifici compiti attribuiti alla Funzione Antiriciclaggio vengono svolti in base a due distinti modelli, declinati per tenere conto dell'articolazione operativa e territoriale del Gruppo stesso. In particolare, si prevede:

- per le Banche e le Società italiane specificamente individuate, la cui operatività è connotata da un elevato livello di integrazione con la Capogruppo, l'accentramento delle attività di presidio dei rischi in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi presso la Direzione Centrale Anti Financial Crime (c.d. modello di gestione accentrata). La scelta di accentramento delle attività è supportata dalla valutazione e documentazione, in una logica di Gruppo, dei rischi, dei costi e dei benefici ad essa associati; tale analisi viene periodicamente aggiornata;
- per le altre Società per cui sussiste un obbligo normativo, nonché per le Filiali Estere, la costituzione di una Funzione Antiriciclaggio e la nomina di un AML Officer, nonché di un Responsabile per la segnalazione di operazioni sospette, cui sono attribuite le responsabilità in materia (c.d. modello di indirizzo, coordinamento e controllo).

Le Società per cui non è richiesta la costituzione della Funzione Antiriciclaggio individuano, ove ritenuto opportuno nel rispetto del principio di proporzionalità, una figura che ha il compito di supportare le Funzioni locali nello svolgimento delle attività di presidio dei rischi di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi, esercitate per le Società italiane nell'ambito del Modello di Organizzazione, gestione e controllo di cui al D. Lgs. n. 231/2001. Tale figura può avvalersi, per eventuali tematiche specifiche, del supporto consultivo della Direzione Centrale Anti Financial Crime.

Nello svolgimento del ruolo di indirizzo, coordinamento e controllo della Capogruppo nei confronti delle Società del Gruppo e delle Filiali Estere, la Direzione Centrale Anti Financial Crime opera in collegamento con le Divisioni, ponendo in essere adeguati scambi informativi e massimizzando le potenziali sinergie. Le Divisioni collaborano con la Direzione Centrale Anti Financial Crime ai fini del recepimento e dell'implementazione da parte delle singole Società e Filiali Estere delle linee guida e delle disposizioni emanate dalla Capogruppo in materia di antiriciclaggio, di contrasto al finanziamento del terrorismo e di gestione degli embarghi, tenendo anche conto dello specifico contesto societario e delle normative locali applicabili.

5.1 Il modello di gestione accentrata

Nelle Banche e Società italiane a cui si applica il modello di gestione accentrata le attività di presidio dei rischi in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi sono svolte dalla Direzione Centrale Anti Financial Crime con il supporto delle altre strutture dell'Area di Governo Chief Compliance Officer. Le attività prestate sono regolate da appositi contratti.

Il Responsabile della Direzione Centrale Anti Financial Crime riveste anche il ruolo di AML Officer per le principali Società su cui è prevista l'applicazione del modello di gestione accentrata. Per le restanti Banche e Società in gestione accentrata, il Responsabile della Direzione Centrale Anti Financial Crime designa un suo rappresentante, in qualità di AML Officer, quale responsabile dello svolgimento in outsourcing dell'attività di presidio dei rischi in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi per conto della Banca o Società controllata. L'AML Officer è designato tra dirigenti o quadri direttivi, in possesso dei requisiti di idoneità previsti dalla normativa vigente, in funzione del ruolo da svolgere per ciascuna Banca o Società che esternalizza l'attività, tenendo conto dei relativi rischi specifici. La nomina, al pari della revoca, dell'AML Officer è sottoposta all'approvazione dell'Organo Societario con funzione di supervisione strategica delle Banche/Società, sentito l'Organo con funzione di controllo²⁰.

Inoltre, in ottemperanza al Provvedimento della Banca d'Italia del 26 marzo 2019, le Banche e le Società in questione nominano un Referente AML, funzionalmente dipendente dall'AML Officer designato, con il compito di supportare la Direzione Centrale Anti Financial Crime nello svolgimento della propria attività, con particolare riferimento all'applicazione alla specifica realtà aziendale delle politiche di gestione dei rischi in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi individuate a livello di Capogruppo, alla gestione delle relazioni con gli Organi Societari ed alla tempestiva segnalazione di eventi o situazioni particolari, suscettibili di modificare i rischi generati dalla controllata.

Il Referente AML deve:

- possedere requisiti di professionalità adeguati;
- essere collocato in posizione gerarchico-funzionale adeguata;
- non avere responsabilità diretta di aree operative sottoposte a controllo né essere gerarchicamente subordinato ai responsabili di tali aree.

La nomina e la revoca del Referente AML sono di competenza dell'Organo Societario con funzione di supervisione strategica delle Banche/Società, sentito l'Organo con funzione di controllo e devono essere sottoposte a parere preventivo del Responsabile della Direzione Centrale Anti Financial Crime.

Con riferimento alle operazioni potenzialmente sospette, le strutture operative delle Banche e delle Società in gestione accentrata effettuano con tempestività la segnalazione di primo livello al Delegato di Gruppo al quale è conferita delega per le segnalazioni delle operazioni sospette con delibera dell'Organo Societario con funzione di supervisione strategica, sentito l'Organo con funzione di controllo. Inoltre, gli Organi con funzione di controllo delle Banche e delle Società in gestione accentrata comunicano al Delegato di Gruppo, ai sensi dell'art. 46, comma 1, lett. a) del D. Lgs. n. 231/2007, le operazioni potenzialmente sospette rilevate nell'esercizio delle proprie funzioni. Il Delegato di Gruppo acquisisce, direttamente o tramite le Banche e le Società, le informazioni utili allo scopo, ivi comprese quelle presenti nell'archivio di conservazione dei dati per l'adempimento degli obblighi antiriciclaggio.

²⁰ In particolare, come previsto dalle "Disposizioni di vigilanza sulla procedura di valutazione dell'idoneità degli esponenti di banche, intermediari finanziari, istituti di moneta elettronica, istituti di pagamento e sistemi di garanzia dei depositanti" di Banca d'Italia, l'Organo con funzione di supervisione strategica valuta, preventivamente alla nomina, il possesso dei requisiti previsti dalla normativa di vigilanza e, fatti salvi i casi di urgenza, trasmette il relativo verbale all'Autorità di Vigilanza competente.

In merito alle infrazioni gravi o ripetute o sistematiche o plurime di cui all'art 46, comma 1, lett. b) e alle infrazioni di cui all'art. 51, comma 1, del D. Lgs. n. 231/2007, le strutture di controllo delle Banche e delle Società in gestione accentrata rilevano e segnalano in tempo utile le medesime alla Direzione Centrale Anti Financial Crime che, attraverso il Responsabile della Funzione e sulla base delle evidenze derivanti dall'attività di controllo di secondo livello svolta, informa gli Organi Societari con funzione di controllo delle Banche e delle Società in gestione accentrata per consentire agli stessi di effettuare la relativa comunicazione all'Autorità di Vigilanza o al MEF; la comunicazione da parte dei predetti Organi deve intervenire anche quando rilevano le infrazioni nell'esercizio dei propri compiti.

5.2 Il modello di indirizzo, coordinamento e controllo

Le Società del Gruppo e le Filiali Estere cui si applica il modello di indirizzo, coordinamento e controllo costituiscono la propria Funzione Antiriciclaggio e nominano, valutando preventivamente il possesso dei requisiti di idoneità previsti dalla normativa di vigilanza ove applicabile, il relativo AML Officer, che generalmente riveste anche il ruolo di Responsabile delle segnalazioni di operazioni sospette, nelle Società italiane sulla base di delega conferita con delibera dell'Organo Societario con funzione di supervisione strategica sentito l'Organo con funzione di controllo e nelle Società e Filiali Estere sulla base dei requisiti previsti dalla normativa locale.

L'AML Officer è collocato in posizione gerarchico-funzionale adeguata, ovvero alle dirette dipendenze dell'Organo Societario con funzione di gestione o dell'Organo Societario con funzione di supervisione strategica e riporta funzionalmente al Responsabile della Direzione Centrale Anti Financial Crime per l'attuazione delle scelte effettuate dalla Capogruppo in materia di politiche, processi e procedure di gestione dei rischi in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi. La nomina, la revoca e gli interventi di riconoscimento meritocratico, in termini di definizione degli obiettivi, valutazione dei risultati e determinazione del bonus, degli AML Officer locali devono essere sottoposti al parere preventivo del Responsabile della Direzione Centrale Anti Financial Crime.

Oltre all'esecuzione dei macro-processi previsti nelle presenti Linee Guida ai fini del presidio e controllo dei rischi in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi, gli AML Officer delle Società del Gruppo e delle Filiali Estere a cui si applica il modello di indirizzo, coordinamento e controllo provvedono a:

- informare la Direzione Centrale Anti Financial Crime, in maniera compiuta e tempestiva, circa gli esiti delle attività di controllo effettuate sulla base di macro-obiettivi di controllo forniti dal Responsabile della Direzione Centrale Anti Financial Crime nonché di ogni accadimento di rilievo. A tal proposito forniscono un reporting semestrale in riferimento alle tematiche disciplinate all'interno dei principi guida dettati dalla Capogruppo²¹;
- proporre e/o condividere le azioni di remediation da intraprendere a fronte di carenze rilevate, definendo le relative tempistiche e responsabilità di attuazione. A tal proposito, con cadenza mensile, informano la Direzione Centrale Anti Financial Crime circa l'avanzamento degli interventi;
- relazionarsi con le Autorità di Vigilanza allo scopo di essere aggiornati sul quadro normativo e di operare in conformità alle disposizioni vigenti relative al modello di business adottato e/o al Paese di insediamento, coordinandosi con la Direzione Centrale Anti Financial Crime nell'ottica di agire in coerenza con le presenti Linee Guida ed agevolare il dialogo con le suddette Autorità. La Direzione Centrale Anti Financial Crime assiste le Società del Gruppo e le Filiali Estere nell'impostazione dei rapporti con le Autorità, ferma restando la responsabilità delle singole Entità nell'attuazione dei requisiti regolamentari specifici del settore di business e/o del Paese di insediamento;

²¹ Tali tematiche possono riguardare, a titolo esemplificativo, evoluzione del contesto normativo locale, numero e tipologia di operazioni segnalate, numero e tipologia di clienti ad alto rischio accettati, interventi formativi pianificati ed erogati, infrazioni alle disposizioni riscontrate, contestazioni ricevute dalle competenti Autorità.

- informare tempestivamente la Direzione Centrale Anti Financial Crime qualora la legislazione locale non permetta l'applicazione delle misure antiriciclaggio, di contrasto al finanziamento del terrorismo e di gestione degli embarghi equivalenti a quelle dell'Unione Europea al fine di consentire al Responsabile della Direzione Centrale Anti Financial Crime di informare la Banca d'Italia, in coerenza con le previsioni del Regolamento Delegato (UE) 2019/758 e per la messa in atto delle misure supplementari, secondo un approccio basato sul rischio.

Agli AML Officer è affidata anche la responsabilità per l'autorizzazione all'esecuzione di un'operazione occasionale o all'apertura e al mantenimento di rapporti in essere con clienti a rischio alto e per la valutazione dei clienti che, in fase di censimento, accensione di rapporti o aggiornamento anagrafico, presentassero un riscontro nelle Sanction List.

Il Responsabile delle segnalazioni di operazioni sospette presso le Società del Gruppo e le Filiali Estere a cui si applica il modello di indirizzo, coordinamento e controllo, provvede a trasmettere al Delegato di Gruppo copia delle segnalazioni inviate all'UIF o alla competente Unità estera²² nonché di quelle archiviate, complete della motivazione che ha determinato l'archiviazione, fatte salve le norme locali in tema di segreto bancario e/o professionale, nonché le ulteriori norme locali che risultino ostative alla trasmissione al Delegato di Gruppo delle suddette segnalazioni. La trasmissione delle informazioni è effettuata con modalità volte a garantire la massima riservatezza dell'identità del Responsabile di primo livello che ha effettuato la segnalazione. Il Delegato di Gruppo, ai fini dell'approfondimento delle operazioni e dei rapporti anomali in un'ottica di Gruppo, si può avvalere di ogni struttura delle entità del Gruppo.

La Direzione Centrale Anti Financial Crime definisce indirizzi di Gruppo e ne presidia la corretta applicazione da parte delle Società e delle Filiali Estere in indirizzo, coordinamento e controllo, secondo il modello definito nelle presenti Linee Guida. A tal fine, con riferimento ai profili connessi alla gestione dei rischi di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi, la Direzione Centrale Anti Financial Crime:

- definisce linee guida e regole metodologiche di Gruppo, individuandone il perimetro geografico e/o di business di applicazione e supportandone a livello locale la relativa applicazione. Tali linee guida e regole metodologiche contengono, tra gli altri, i principi generali o comunque gli standard minimi di comportamento da seguire in tema di:
 - obblighi di adeguata verifica (set informativo e metodologia per procedere all'adeguata verifica della clientela e alla revisione del profilo di rischio della medesima nonché criteri per l'accettazione della clientela e obblighi di astensione);
 - obblighi di conservazione e messa a disposizione dei dati (modalità di conservazione dei dati e per la messa a disposizione dei dati alle Autorità, gestione delle informazioni e della documentazione acquisita dalla clientela);
 - processi e procedure da adottare nell'ambito del monitoraggio delle operazioni effettuate dalla clientela;
 - processi e procedure per il presidio in ambito embarghi con particolare riferimento alla definizione delle Sanction List e degli obiettivi di controllo;
 - processi e procedure per il presidio in ambito antiterrorismo con particolare riferimento alla definizione delle liste e degli obiettivi di controllo;
 - obblighi di segnalazione (modalità di valutazione delle operazioni potenzialmente sospette ai fini dell'eventuale segnalazione di primo livello nonché tempestività della segnalazione, tracciabilità dell'iter valutativo, identificazione chiara delle responsabilità);
 - limitazioni all'uso del contante e dei titoli al portatore;
 - formazione del personale (tipologia di iniziative da erogare, contenuti minimi delle stesse e utenti a cui rivolgerle);
 - sistema dei controlli (macro-obiettivi di controllo, tipologia e modalità di conduzione dei controlli);

²² L'art. 33, comma 2, della Direttiva (UE) 2015/849 dispone che il soggetto obbligato alla segnalazione di operazione sospetta trasmetta le informazioni all'Unità dello Stato membro presso cui è situato.

- supporta gli AML Officer locali nell'elaborazione dei risk assessment e ne analizza gli esiti, al fine di favorire l'omogeneità delle valutazioni e pervenire ad una visione d'insieme dei rischi e dei presidi a livello di Gruppo, ed elabora in logica risk-based il piano annuale degli interventi delle attività di indirizzo, coordinamento e controllo;
- verifica, di concerto con gli AML Officer, la possibilità di estendere i Key Risk Indicator quantitativi rilevanti per il monitoraggio dei rischi di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi alle Società e alle Filiali Estere, supporta quest'ultime, in caso di superamento delle soglie fissate, nell'identificazione e analisi degli eventi ascrivibili alla mancata conformità alle norme e degli opportuni interventi di mitigazione e attiva, laddove necessario, i meccanismi di escalation previsti dalle Linee Guida sul RAF;
- definisce - nell'ambito di iniziative progettuali di gestione dei rischi in materia di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi a valere sul Gruppo - processi operativi e relativi strumenti a supporto, coordinandone la fase realizzativa a livello locale;
- fornisce supporto tecnico alle Società e Filiali Estere e attiva - su richiesta discrezionale di una qualsiasi delle strutture valutatrici a livello locale - il processo di valutazione preventiva, nel contesto dei relativi processi di Product Governance e clearing, coinvolgendo le competenti strutture di Capogruppo;
- indirizza le Società e le Filiali Estere nello sviluppo di metodologie e modelli di controllo omogenei, ed effettua - anche mediante verifiche in loco - la verifica dell'adeguatezza e dell'effettiva applicazione dei presidi definiti a livello di Gruppo;
- coordina le iniziative di formazione - verificandone la coerenza e le sinergie con le iniziative adottate a livello di Capogruppo - e promuove giornate e/o eventi di incontro con gli AML Officer locali;
- supporta gli AML Officer locali nel riscontro alle Autorità di Vigilanza, concorrendo alla definizione dei piani di remediation e monitorandone la relativa attuazione;
- supporta, su richiesta, gli AML Officer locali nella predisposizione dei flussi informativi agli Organi Societari.

Per lo svolgimento dei propri compiti la Direzione Centrale Anti Financial Crime ha accesso a tutte le attività delle Società del Gruppo e delle Filiali Estere in questione, nonché a qualsiasi informazione rilevante con riferimento ai rischi di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi, anche attraverso il colloquio diretto con il personale.

Le Società del Gruppo e le Filiali Estere a cui si applica il modello di indirizzo, coordinamento e controllo sono tenute a:

- recepire, per le Società con approvazione da parte degli Organi Sociali, le linee guida e le regole emanate dalla Capogruppo in tema di gestione dei rischi di riciclaggio, di finanziamento del terrorismo e di violazione degli embarghi, adeguandole, ove necessario, in coordinamento con la Direzione Centrale Anti Financial Crime, al proprio contesto e alle specificità delle normative locali;
- fare propri gli standard operativi di lavoro e le metodologie definiti dalla Direzione Centrale Anti Financial Crime, raccordandosi con la stessa per gli eventuali adattamenti alle specifiche realtà aziendali; in particolare, nel caso di controllate estere, devono essere adottate tutte le iniziative atte a garantire standard di controllo e presidi comparabili a quelli previsti dalle Disposizioni di vigilanza italiane, anche nei casi in cui la normativa dei Paesi in cui sono insediate le filiazioni non preveda analoghi livelli di attenzione;
- fornire alla Direzione Centrale Anti Financial Crime con riferimento all'ambito antiriciclaggio, contrasto al finanziamento del terrorismo ed embarghi i flussi informativi definiti nell'Allegato B delle Linee Guida di Compliance di Gruppo, garantendo altresì tempestiva informativa in caso di eventi che possano determinare l'emersione di rischi connessi a tale ambito.

Le Società del Gruppo che detengono a loro volta, direttamente o indirettamente, partecipazioni di controllo, sono tenute ad individuare il più idoneo modello organizzativo per le controllate appartenenti al proprio perimetro di competenza, concordandolo con la Direzione Centrale Anti Financial Crime. Esse sono altresì responsabili della diffusione presso le controllate delle linee guida

emanate dalla Capogruppo e della verifica del loro corretto recepimento ed applicazione²³. I flussi informativi inviati a Capogruppo devono garantire idonea conoscenza della realtà in essere presso le controllate con riferimento ai rischi in materia di antiriciclaggio, contrasto al finanziamento del terrorismo e gestione degli embarghi.

²³ Le Società del Gruppo, nel recepire le presenti Linee Guida, descrivono il modello organizzativo individuato per le controllate appartenenti al proprio perimetro.