POLITICA ANTIRICICLAGGIO

BNP Paribas Cardif Vita SpA

Ai sensi dell'articolo 10, comma 1, lettera b) del Regolamento IVASS n. 44 del 12 febbraio 2019 e s.m.i.

PER USO INTERNO

Versione 7 [26/09/2024]

BNP PARIBAS CARDIF

The insurer for a changing world

QUADRO GENERALE DELLA POLITICA

Owner*	Compliance			
Processi impattati*	PR00005 - Compliance	Select an item.	Select an item.	Others

Livello	Livello 3
Tipologia documento*	Politica
Ambito di applicazione*	Cardif Vita (132 007)
Da adattare localmente*	Specifica
Classificazione*	Interna
Accesso	Tutto il personale
Autore	V. Becchi
Unità organizzativa dell'autore*	Compliance
Organo responsabile per l'approvazione*	Consiglio di Amministrazione
Contributors*	Internal Audit, Customer Service, Process Engineering, Human Resources, OPC, Governance Management, Data Office

Codice*	IT-CPL-10-IT
Versione*	7.0
Data di Validazione*	26/09/2024
Data di efficacia*	26/09/2024
Frequenza di revisione	Annuale

Norme correlate	- Reg. IVASS n. 44 del 12 febbraio 2019 - Provvedimento IVASS n. 111 del 13 luglio 2021 - D. Lgs. 231/2007 e D. Lgs. 109/2007, entrambi modificati dal D. Lgs. 90/2017 - in recepimento del cd. "IV Direttiva UE" (i.e. Dir. n. 849/2015 – D. Lgs. N. 90/2017) - D. Lgs. N. 125/2019 in recepimento della cd. "V Direttiva UE" (i.e. Dir. n. 843/2018) - D. Lgs. 195/2021 in recepimento della cd. "VI Direttiva UE" (i.e. Dir. n. 2018/1673) - Decreto 11 marzo 2022, n. 55 del Ministero dell'Economia e delle Finanze - Regolamento n. 2580/2001 del Consiglio dell'Unione Europea del 27 dicembre 2001 (Artt. 318 e ss. c.p.; Art. 2635 c.c.) - D. Lgs. 231/01 del 8 giugno 2001 - L. n. 190/2012 - Orientamenti europei EBA - Provvedimento IVASS n. 144/2024
Documenti correlati	- Modello di Organizzazione, Gestione e Controllo ex D.Lgs 231/01 - IT-GOV-05-IT Conduct Policy - INS-CPL-FS01-V11Global Anti-Money Laundering & Counter Terrorist Financing (AML-CTF) Policy - IT-CPL-24-IT v.4 Know Your Client - Global Policy (KYC) - IT-CPL-46-ITOperazioni Sospette di riciclaggio e/o connesse al terrorismo

	- IT-CPL-43-IT Linee Guida per l'adozione di misure di asset Freeze - IT-CPL-44-IT Tenuta AUI: Rapporti Continuativi e Operazioni Monetarie - IT-CPL-23-IT Politica applicabile alle relazioni con Persone Politicamente Esposte (PEP) - CPL0253-HO Group Know Your Client - Segment Corporates & Small Businesses - CPL0260-HO Group Know Your Client - Segment: Private Investment Vehicles (PIVs) - CPL0266-HO Group Know Your Client - Segment: Retail Markets & Private Banking - CPL0269-HO Group Know Your Client - Segment: Nonprofit Private Entities - INS-CPL-FS44-HO Group Policy on international financial sanctions & embargoes training - IT-CPL-42-IT Policy sulla formazione in materia antiriciclaggio e contrasto al finanziamento del terrorismo - IT-CPL-26-IT Erogazione formazione Compliance e Sicurezza Finanziaria al personale - INS-CPL-FS35-HO Global Sanctions Policy - IT-CPL-04-IT Country Policy - Policy applicabile alle attività relative ai Paesi in cui BNP Paribas non ha presenza fisica - CAN 03-02-03 MSCQ Process - INS-CPL-FS36-HO Screening of Relationships - INS-CPL-FS42-HO Sanction Advisory Routing and Decision Process - INS-CPL-FS20-HO Procedure for the escalation of sanctions transactional inquiries - IT-CPL-15-IT Politica globale contro il finanziamento del terrorismo - IT-CPL-13-IT Monitoraggio delle Transazioni e Gestione degli Alert (AML_TM) - INS-CPL-FS39-HO Cuba Policy - INS-CPL-FS40-HO Procedure concerning Ukraine/Russia-related sectoral sanctions - INS-CPL-FS41-HO Relationships involving individual nationals and residents of the MSCs (and Regions) of Iran, Syria, North Korea, and Crimea/Sevastopol - IT-CPL-21-IT Politica Anticorruzione - IT-CPL-30-IT CAC Policy - IT-CPL-31-IT Circumvention Procedure - CAN 03-03-04 Recusal Policy - US Person - IT-CPL-45-IT Voluntary Self Disclosure - IT-CPL-20-IT Know Your Intermediary - IT-CPL-28-ITAllerta Etico - IT-PROC-01-IT Acquisti di Beni e Servizi e Gestione di Fornitori - IT-OPS-29-IT SUN Fircosoft

Parole chiave	Antiriciclaggio, Antiterrorismo, operazioni sospette, adeguata verifica, sanzioni internazionali
Sintesi	La Politica Antiriciclaggio viene predisposta, validata e periodicamente aggiornata, in attuazione dell'articolo 10, comma 1, lettera b) del Regolamento IVASS n. 44 del 12 febbraio 2019 (come modificato dal Provvedimento IVASS n. 111/2021 nonché in conformità al Provv. n. 144/2024), al fine di determinare le regole, i principi generali e le conseguenti azioni conformi alla normativa - tempo per tempo in vigore – utili ad identificare e gestire i rischi connessi con il riciclaggio ed il finanziamento del terrorismo per Cardif Vita S.p.A.

**campi obbligatori*

STORICO VERSIONE/ MODIFICHE APPORTATE

N. versione	Data entrata in vigore	Descrizione della modifica	Autore della modifica
V3	24/09/2019	Prima adozione ai sensi del Regolamento 44 / 2019	V. Becchi
V3	18/09/2020	Revisione annuale	V. Becchi
V4	22/07/2021	Revisione annuale	V. Becchi
V5	25/07/2022	Revisione annuale	V. Becchi
V6	20/07/2023	Revisione annuale	V. Becchi
V7	26/09/2024	Revisione annuale	V. Becchi

Indice

1. Normativa di riferimento ambito di applicazione e obiettivi della politica antiriciclaggio

1.1 Ambito generale di applicazione

La Politica Antiriciclaggio (anche "Politica AML" o "Policy AML") viene predisposta, validata e periodicamente aggiornata, in attuazione dell'articolo 10, comma 1, lettera b) del Regolamento IVASS n. 44 del 12 febbraio 2019 (come modificato dal Provvedimento IVASS n. 111/2021 e dal Provvedimento IVASS n. 144/2024[1]), al fine di determinare le regole, i principi generali e le conseguenti azioni conformi alla normativa - tempo per tempo in vigore – utili ad identificare e gestire i rischi connessi con il riciclaggio ed il finanziamento del terrorismo per Cardif Vita S.p.A. (anche "Cardif Vita" o la "Compagnia").

La Politica AML recepisce le linee strategiche e le indicazioni in materia di gestione del rischio di riciclaggio e contrasto al finanziamento del terrorismo che per la Compagnia vengono, in primo luogo e conformemente ad una procedura di gestione del rischio globale e di Gruppo (internazionale nel caso di specie – rif. BNP Paribas), stabilite tramite la "*Global Anti-Money Laundering & Counter Terrorist Financing (AML-CTF) Policy*" di BNP Paribas Cardif (di seguito anche "Policy AML di Gruppo"), nell'ambito della direzione e coordinamento da questa esercitata, quindi, conseguentemente implementate localmente mediante ogni necessario e/o opportuno adeguamento (rif. Allegato 1).

Nell'ambito del nuovo contesto normativo di antiriciclaggio (infra "AML") delineato a seguito del progressivo recepimento della (I) cd. "IV Direttiva UE" (i.e. Dir. n. 849/2015 – D. Lgs. N. 90/2017) quindi della (II) cd. "V Direttiva UE" (i.e. Dir. n. 843/2018 – D. Lgs. N. 125/2019) nonché della (III) cd. "VI Direttiva UE" *(*i.e. la Direttiva (UE) 2024/1640 del 31 maggio 2024 relativa ai meccanismi che gli Stati membri devono istituire per prevenire l'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo, che modifica la Direttiva (UE) 2019/1937, e abroga la direttiva (UE) 2015/849– con intervento del Legislatore a livello penale già mediante D. Lgs. 195/2021[2]), al fine di determinare regole e principi che siano riferiti a un contesto il più possibile completo, armonizzato ed anche efficace, la presente Politica AML tiene conto di:

- standard internazionali e fonti normative comunitarie (cfr. "*Linee Guida sulla cooperazione e sullo scambio di informazioni tra le Autorità di vigilanza in materia di antiriciclaggio*" emanate da EBA-ESMA ed EIOPA, *Linee Guida* sugli obblighi di adeguata verifica della clientela e sui fattori che gli enti creditizi e finanziari devono considerare nel valutare il rischio di riciclaggio e di finanziamento del terrorismo associato ai singoli rapporti d'affari e alle operazioni occasionali ai sensi degli articoli 17 e 18, paragrafo 4, della Direttiva (UE) 2015/849*" (le cc.dd. "*CDD and Risk Factor Guidelines*")* considerati anche quali principi cogenti, sia in virtù dell'adesione dell'Italia al "TFUE[3]" (Trattato di Funzionamento dell'Unione Europea) sia anche per quanto richiamati dalla regolamentazione secondaria e attuativa degli adempimenti di Legge*;*
- fonti nazionali di primo livello e regolamentari di attuazione;
- indicazioni da parte delle associazioni di categoria (ANIA) - quali utili chiarimenti e/o interpretazioni agli obblighi in vigore;

nonché, essendo la Compagnia parte di un Gruppo a livello internazionale anche delle

- disposizioni dettate dal Gruppo a livello globale (quali criteri suppletivi e integrativi ove di maggior rigore).

[1] La presente versione della Politica include solo parzialmente le novità introdotte dal Provvedimento 144/2024, in quanto ricomprende solo i presidi già implementati o in fase di prossima messa a terra. Verrà pertanto rivista via via che ulteriori presidi saranno implementati.

[2] Integrante gli aspetti di Diritto penale della V Direttiva con norme minime di miglior raccordo della definizione dei reati e delle sanzioni in materia di riciclaggio.

[3] Art. 114 T.F.UE.

In conformità con quanto previsto dalla normativa, tempo per tempo, vigente (attualmente articolo 10, comma 1, lettera b) del Regolamento IVASS n. 44), la Politica AML individua e determina le scelte assunte da Cardif Vita in materia di antiriciclaggio ("**AML**") e di contrasto al finanziamento del terrorismo e alla conformità all'osservanza delle sanzioni internazionali ("**CTF**") al fine di garantire un efficace riduzione del rischio.

L'adozione di un approccio basato sul contenimento del rischio ("*risk based approach*") è da considerare quale risultante, oltre che degli adeguamenti normativi, anche dell'esito dei controlli e delle misure di presidio predisposte a mitigazione dei rischi, con l'effetto che la presente Politica AML è dipendente da aggiornamenti in funzione di tali "fattori".

In dettaglio, avendo a riferimento la struttura organizzativa, i rischi, gli adempimenti/obblighi, nonché le necessità di controllo, la Politica AML detta disposizioni vincolanti nell'ambito di:

- **assetti organizzativi**, sia in riferimento alla struttura organizzativa che ricomprende - nei vertici aziendali - l'Organo di supervisione Strategica (Consiglio di Amministrazione) e l'Organo con funzione di gestione (con declinazione dei relativi requisiti e compiti) sia alle connesse titolarità e responsabilità della Funzione Antiriciclaggio (con responsabilità e compiti non esternalizzabili, salve specifiche attività), con espressa previsione di un sostituto del titolare, e la valutazione e gestione degli aspetti segnaletici (i.e. Delegato SOS) ivi inclusi i processi afferenti ai flussi informativi tra le funzioni di controllo, nonché di selezione e/o comunicazione/notifica verso le Autorità di Vigilanza di settore (i.e. IVASS) delle criticità sostanziali rilevate dai controlli interni (in ragione delle risultanze delle verifiche periodiche e/o a evento);
- **adempimenti AML e CTF** (e relativi adempimenti e processi aziendali)
  - **adeguata verifica**, sia in riferimento ai principi generali per l'acquisizione dei dati e delle informazioni considerate essenziali ai fini della instaurazione del rapporto, sia anche sotto il profilo dell'aggiornamento e/o della modifica e attivazione di "misure rafforzate" (in particolar modo per la clientela classificata ad "alto rischio") anche per beneficiari e/o legami di titolarità effettiva che riconducano a Paesi ad "alto rischio";
  - **conservazione dei dati** (per come, tempo per tempo, applicabile ai sensi delle disposizioni regolamentari) anche in caso di, eventuale, operatività transfrontaliera[4];
  - **individuazione delle operazioni sospette e delle procedure (anche a intendersi quali misure rafforzate e/o istruzioni al personale) previste per l'individuazione e la relativa segnalazione anche nella cooperazione con altri Intermediari – facenti parte della rete distributiva diretta -** (anche in riferimento alle nuove casistiche e/o fattori di rischio individuati dalla UIF nei propri schemi di anomalia o nell'ambito di circolari o nella Relazione Annuale sull'attività svolta);
  - **formazione del personale**.

Quanto precede, sotto un profilo di mitigazione dei rischi, altresì considerando:

- le **procedure di selezione e accertamento dei requisiti del Responsabile della Funzione Antiriciclaggio**;
- l'esistenza e il mantenimento dei **requisiti di professionalità, onorabilità e autonomia e indipendenza - gerarchica e/o operativa** - in capo al **Responsabile della Funzione Antiriciclaggio** (nonché soggetto delegato per la segnalazione delle operazioni sospette) – e **relativo sostituto** ("**Deputy**") nei casi, anche temporanei, di impedimento - da possedere sia al momento dell'assunzione dell'incarico sia in linea di continuità operativa, le relative e correlate procedure di valutazione, la descrizione delle situazioni che comportano una nuova valutazione (cd. rinnovazione e/o conferma) dei requisiti e la procedura per notificare (o confermare) all'IVASS il Responsabile della Funzione.
  Requisiti per i quali vengono effettuati puntuali e continui controlli di sussistenza che, in caso di ogni ed eventuale sopraggiunta carenza, determinano una specifica evidenziazione per la sottoposizione a valutazione e determinazione delle misure correttive del caso.
  Quanto precede, anche a precisare e così significare che l'assenza integrale di elementi o riscontri di potenziale carenza e/o di sopraggiunta inidoneità, anche parziale, per la stessa configurazione dei poteri delegati attribuiti, può non richiedere una specifica formalizzazione.

[4] Che deve avvenire sempre nell'ambito dei requisiti autorizzativi che consentono l'esercizio all'attività assicurativa in Italia.

1.2 Normativa di riferimento

Nell'individuare la normativa di riferimento, idonea all'efficace contrasto del riciclaggio di capitali e del finanziamento del terrorismo, si deve necessariamente avere a riferimento l'ampia definizione amministrativa prevista dal legislatore.

Nell'ambito del cd. "*framework* normativo AML di riferimento" cui la Compagnia si riferisce, vengono incluse sia le attività illecite[5] che possono cagionare l'occultamento (anche sotto forma di tentativo) dell'origine illecita dei fondi, insite nell'apertura di rapporti e/o nel compimento di operazioni, sia anche ogni condotta che possa causare o abbia la finalità di re-investimento dei proventi illeciti (derivanti da reato, anche contravvenzionale ivi compresa la forma del tentativo e di auto-riciclaggio, pertanto, da includere nella categoria più ampia ed estesa riferibile al "sospetto" che prescinde da un accertamento sostanziale della illiceità) in attività legali (antiriciclaggio "AML") e/o l'utilizzo di capitali leciti per finanziare attività illecite (contrasto al finanziamento del terrorismo "CTF").

Ne consegue che risulta così richiamata e ritenuta applicabile ogni norma, provvedimento, interpretazione autentica anche estensiva che sia o si ritenga applicabile a livello internazionale, comunitario, ovvero nazionale, in quanto emanato da Autorità Legislative e/o regolamentari di settore.

Trattandosi di operatività locale svolta da entità italiane che, tuttavia, devono uniformarsi anche ai principi generali di Gruppo, la Politica AML si deve considerare:

(1→) in conformità e armonia con i principi e le regole previste dalla normativa antiriciclaggio e a contrasto del finanziamento del terrorismo nella formulazione, tempo per tempo vigente, quindi, inclusiva di ogni normativa correlata e/o di raccordo (ad es. normativa anticorruzione e/o adempimenti e/o segnalazioni a contrasto dell'evasione fiscale internazionale). Attualmente, il D. Lgs. 231/2007 e ss. m. e i. ("**AML**") e il D. Lgs. 109/2007 e ss. m. e i. ("**CTF**"), entrambi modificati dapprima (I) dal D. Lgs. 90/2017[6] entrato in vigore il 4 luglio 2017- (in recepimento della "IV Direttiva"), quindi (II) dal D. Lgs. 125/2019 entrato in vigore il 10 novembre 2019 (in recepimento della "V Direttiva") nonché (III) dal D. Lgs. 195/2021 entrato in vigore il 15 dicembre 2021 (in recepimento della "VI Direttiva) e relative disposizioni di attuazione emanate dalle Autorità di vigilanza di settore (i.e. IVASS) nonché dalle disposizioni di interpretazione autentica emanate dal Ministero dell'Economia e dall'Unità di Informazione Finanziaria (di seguito anche "UIF");

(2→) è da intendersi in ogni caso soggetta – per quanto applicabili - ai principi, criteri e alle regole previste a livello locale (i cd. "*local requirements*").

Quanto precede (i) in conformità a quanto concordato a livello internazionale e di Gruppo, le cui regole, nel caso, dovranno intendersi come prevalenti ove più stringenti e/o rigorose e/o richiedenti un livello di dettaglio superiore in termini di dati, informazioni, documenti e/o controlli; (ii) con l'espresso limite che l'applicazione non si ponga in contrasto con norme inderogabili di legge e/o provvedimenti dell'Autorità di Vigilanza disposti anche a livello di Gruppo.

La declinazione degli obblighi deve ritenersi incentrata su aspetti di "prevenzione" e di "ponderata valutazione" di ogni evento di rischio insiti: **(A)** anzitutto, in una **adeguata classificazione della clientela** (ai fini di ogni debita e/o pertinente attività di preliminare verifica e di conseguente controllo e rinnovazione della "adeguata verifica" anche ai fini dell'aggiornamento della profilatura - inclusivi anche degli obblighi di astensione in caso di mancata comunicazione da parte del Cliente e/o acquisizione da parte della Compagnia di dati essenziali per il compimento della "adeguata verifica"-) e/o in **(B)** ogni attività idonea ad una **segnalazione delle operazioni sospette** (inclusiva degli **obblighi di astensione in ragione di (B.1) elevati rischi o sospetti di coinvolgimento in attività di potenziale riciclaggio o finanziamento del terrorismo**; anche conseguenti **(B.2) all'assolvimento di ogni attività e/o adempimento utile a consentire l'emissione di provvedimenti amministrativi e cautelari a seguito di istanza *ex* art. 6 co. 4 D. Lgs. Cit.**) da applicarsi anche nell'ambito della cooperazione con altri Intermediari della "rete distributiva", oltre che di **(C)** adozione delle **misure di congelamento e dei conseguenti obblighi di comunicazione**, disciplinate in materia di contrasto al terrorismo (incluso il Regolamento n. 2580/2001 del Consiglio dell'Unione Europea del 27 dicembre 2001) ed ogni misura restrittiva a ritenersi applicabile (i.e. misure restrittive dell'operatività internazionale), tra le quali le disposizioni emanate contro determinate persone e entità.

[5] Il riferimento è al sospetto di provenienza illecita, anche nella forma del tentativo e ricomprende anche "adverse news".

[6] Ogni riferimento al D. Lgs. 231/2007 e al D. Lgs. 109/2007 si intende comprensivo delle modifiche apportate dalle disposizioni normative - tempo per tempo - sopraggiunte.

Trattandosi di attività di "prevenzione" strutturata su "anomalie" che, laddove individuate e non giustificate, divengono "sospetto", deve ritenersi richiamata e applicabile, tempo per tempo, anche ogni disposizione normativa che abbia la finalità di contrastare e reprimere, oltre ai cd. "**reati presupposto" anche i principali "eventi di rischio**" che possono, quale anomalia, degenerare in un sospetto di riciclaggio (inteso in rapporto all'ampia definizione di cui all'art. 2 D. lgs. N. 231/07)[7].

Il riferimento per l'inclusione nel perimetro applicativo di qualsiasi attività potenzialmente illecita e/o non conforme ad etica e correttezza (anche di disposizioni regolamentari e/o aziendali -incluso il Codice di Condotta), oltre ovviamente che riconducibili alla commissione di potenziali reati, si estende e include anche le disposizioni a contrasto della **corruzione** (artt. 318 e ss. c.p.) compresa quella internazionale e/o tra "privati" (cfr. art. 2635 c.c.), nonché quanto riferito alle disposizioni a "**contrasto della evasione fiscale**" dettate dalla normativa nazionale ed internazionale.

Quanto precede, si deve intendere non solo quale adozione di misure a contrasto del rischio associabile alle categorie di clienti, individuati dalla normativa, a "maggior rischio intrinseco" (ad es. "PEPs" - Persone Politicamente Esposte - e "PIL" - Politici Italiani locali/Persone Localmente Importanti -), nonché quelle categorie "integrative" (anche riferite ai prodotti) e/o i clienti classificati dalla Compagnia a "maggior rischio"; per l'effetto, si prenderà in considerazione anche il verificarsi di condotte nelle quali vi siano offerte di vantaggi o oggetti di valore, a persone che rivestono cariche pubbliche o private o a terze parti, compreso il caso in cui venga individuata la finalità di ottenere o mantenere il proprio *business* ovvero acquisire un beneficio non dovuto o conseguire un vantaggio anche non patrimoniale (cfr. anche L. n. 190/2012).

Per il loro carattere di "trasversalità" su tutte le attività della Compagnia, le misure della Politica AML costituiscono anche, principi e regole per un efficace presidio del rischio di riciclaggio e di finanziamento del terrorismo anche per:

(→) il **Modello Organizzativo, di Gestione e Controllo *ex* D. Lgs. n. 231/2001 della Compagnia** (*cfr.* **D. Lgs. 231/2001** recante disposizioni in materia di "disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300" che mutua i presidi a contrasto del riciclaggio e del finanziamento del terrorismo;

(→) le determinazioni circa il perseguimento dell'oggetto statutario e la validazione di nuove attività e/o prodotti, sotto il profilo della preventiva analisi dei rischi (cd. "AML *by design*").

Nell'ambito della declinazione, interpretazione e aggiornamento, della Politica AML, coerentemente con gli Orientamenti europei EBA[8], le normative di gruppo e nazionali, il criterio principale sarà sempre il perseguimento e l'applicazione dell'**approccio basato sul rischio** (cd. **"*risk based approach*"**) che chiede alle **imprese e agli intermediari assicurativi** di farsi **parte attiva** nell'**individuazione** e nella **valutazione preventiva dei rischi** di riciclaggio e finanziamento del terrorismo ai quali sono in concreto esposti e nella scelta delle misure più adeguate a fronteggiarli.

Ne consegue come la presente Politica AML" stabilisca i seguenti criteri generali:

(→) il "***risk based approach***" costituisce il criterio necessario per garantire un'efficace e conforme attuazione degli adempimenti AML e CTF anche per l'**acquisizione** di dati e informazioni (anche integrativi) da raccogliere sulla **natura e lo scopo del rapporto continuativo**, nonché sui **soggetti coinvolti** nel rapporto, includendo **misure rafforzate di adeguata verifica**, in caso di individuazione di un **elevato rischio di riciclaggio** (come da previsioni normative ovvero dall'autonoma valutazione della Compagnia);

(→) il **riporto informativo costante verso il Consiglio di Amministrazione e l'Organo con funzione di gestione** da parte del **Responsabile della Funzione Antiriciclaggio**;

(→) la "**coerenza**" al rischio calcolato e assegnato, tempo per tempo, individuato quale condizione essenziale per poter applicare **misure di adeguata verifica semplificata** che si traduce in una riduzione dell'estensione o della frequenza degli adempimenti previsti per **rapporti continuativi ed operazioni a basso rischio, oltre che la "coerenza" nell'assolvimento degli altri obblighi e/o adempimenti (ad es. comunicazioni e/o segnalazioni effettuate per finalità fiscali)**;

[7] Si segnala che a seguito dell'entrata in vigore del D. Lgs. 195/2021 in attuazione della VI Direttiva UE le condotte costitutive dei reati di riciclaggio ed autoriciclaggio possono provenire da qualsiasi delitto nonché da contravvenzioni punite con l'arresto superiore nel massimo ad un anno o nel minimo a sei mesi.

[8] Come tempo per tempo vigenti (cfr. da ultimo EBA/GL/2023/03).

(→) un "**costante monitoraggio**" conformemente alla classificazione di rischio di ogni rapporto tenuto dai Clienti, anche ai fini dell'individuazione di scostamenti sostanziali e/o significativi in termini di incremento dei rischi;

(→) l'"**armonizzazione**" e l'"**omogeneità**" delle misure con quelle di Gruppo, nel rispetto della normativa locale e dei principi inderogabili;

(→) un "**periodico e costante aggiornamento**" sia con le disposizioni regolamentari (i.e. IVASS con l'adozione delle disposizioni sui fattori di rischio, sulle procedure di mitigazione del rischio e sulla conservazione di dati e informazioni in archivi informatici) che con l'esito dei controlli.

2. Approvazione e revisione della politica AML

La Politica AML approvata dal Consiglio di Amministrazione della Compagnia[9], viene definita e aggiornata in coerenza con gli orientamenti strategici adottati in materia di gestione del rischio di riciclaggio, oltre che di conformità normativa, per l'effetto, deve risultare sempre adeguata all'entità e alla tipologia del rischio cui è esposta l'impresa. Rischio complessivo che viene determinato, anche a seguito dell'esercizio di autovalutazione, su base annuale e con possibilità di aggiornamento periodico, inclusivo di tutti i fattori di rischio per Cliente (tipologia o classi di); Prodotto; Rete/Canale Distributivo; Operazioni; Paesi Terzi (rif. flussi monetari o legami dei Clienti con).

Conseguentemente, ne è disposto un aggiornamento su base "almeno annuale", salvo la necessità, in virtù di novità regolamentari e/o dei risultati dell'esercizio di autovalutazione del rischio di riciclaggio, oltre che di ogni altro fattore anche afferente all'evoluzione dell'operatività aziendale, di procedere anticipatamente ad un adeguamento della stessa.

È determinato che la Politica AML è e rimane in vigore nel documento aggiornato sino all'approvazione delle modifiche che, ove non sostanziali, possono essere assunte mediante provvedimento della Funzione Antiriciclaggio e portate a conoscenza del Consiglio di Amministrazione della Compagnia affinché vengano approvate in occasione della prima sessione utile.

In conformità con quanto previsto dall'articolo 14, comma 2, lettera k) del Regolamento IVASS n. 44/19, la Funzione Antiriciclaggio è la funzione aziendale deputata a concorrere a predisporre e aggiornare la Politica e a diffonderla a tutto il personale e, qualora presente, alla rete distributiva diretta, mediante apposite modalità (i.e. sia a mezzo di specifiche comunicazioni riportanti le principali novità sia anche, periodicamente, attraverso appositi strumenti formativi).

Per una adeguata implementazione e rigorosa osservanza, oltre che ai fini della conoscenza di ogni ed eventuale modifica intervenuta in aggiornamento, la Politica AML viene altresì pubblicata sulla Echonet aziendale.

[9] In qualità di organo amministrativo cui è attribuita la funzione di supervisione strategica.

3. Modello di governo del rischio di riciclaggio e di finanziamento del terrorismo

3.1 Principi generali

La Compagnia si è dotata e mantiene un sistema di governo societario e dei rischi (AML e CTF) adeguato alla propria natura e dimensione, in conformità con quanto previsto dai Regolamenti IVASS n. 38 del 3 luglio 2018 e n° 44 del 12 febbraio 2019 così come modificato ed integrato dal Provvedimento IVASS n. 111 del 13 luglio 2021, nonché alla natura, portata e complessità del rischio di riciclaggio come risultante dall'esercizio di autovalutazione, ovvero di ogni indicazione che sia specificatamente indirizzata alla Compagnia da parte delle Autorità di Vigilanza.

In tale contesto, la Compagnia procede e prosegue nel continuo a identificare e a conferire centrale rilevanza alle regole applicabili per effettuare una adeguata classificazione del rischio di riciclaggio nelle proprie direttrici principali (ad es. per clienti, controparti, prodotti, Paesi, canali distributivi) che risulti coerente con la politica di gestione del rischio di Gruppo, le relative strategie applicabili nonché con la normativa locale.

I principi "cardine" del modello di governo del rischio di riciclaggio e contrasto al finanziamento del terrorismo sono i seguenti:

- assegnazione dei compiti all'Organo con funzione di gestione affinché, in conformità all'art. 11 del Regolamento n. 44/2019 IVASS, curi l'attuazione degli indirizzi strategici e della politica di gestione del rischio di riciclaggio definiti dall'organo amministrativo; nonché l'adozione degli interventi necessari ad assicurare l'efficacia nel tempo dell'organizzazione, del sistema dei controlli antiriciclaggio e i flussi informativi.

- istituzione e mantenimento di una Funzione Antiriciclaggio con nomina di un Responsabile della Funzione Antiriciclaggio e attribuzione e aggiornamento dei compiti, in funzione dell'evoluzione sia (a) normativa; sia (b) dei rischi; con nomina del relativo sostituto per la continuità di funzione aziendale, da assolvere nei casi di impedimento, anche temporaneo. A seguito della, preventiva, valutazione e determinazione di miglior assetto organizzativo attraverso la coincidenza del Responsabile della Funzione Antiriciclaggio con il Delegato per la Segnalazione di Operazioni Sospette (anche "Delegato SOS"), individuazione e nomina mediante apposito conferimento di delega e attribuzione di compiti del Responsabile/ Delegato SOS;

in dettaglio, attraverso l'assetto di governance sopra delineato, mediante

- esecuzione di analisi e valutazione dei rischi di riciclaggio e di finanziamento del terrorismo e adeguamento delle procedure in coerenza con i criteri e le metodologie definite;

- modulazione dell'intensità e dell'estensione delle attività e dei controlli posti in essere secondo il grado di rischio di riciclaggio associato alla clientela nel rispetto dell'approccio basato sul rischio, nonché sulla base del grado di (i) esposizione complessiva ai rischi di riciclaggio e di finanziamento del terrorismo che emerge conducendo annualmente l'esercizio di autovalutazione; (ii) modifica dei rischi sostanziali, anche in riferimento ai singoli fattori di rischio considerati nell'ambito dell'esercizio di autovalutazione;

- impegno ad agire sempre in conformità alle norme volte a contrastare il fenomeno del riciclaggio di denaro ed il finanziamento del terrorismo, nel rispetto degli standard definiti dal Gruppo per come declinati a livello locale;

- definizione di sistemi valutativi e processi operativi chiari, oggettivi, periodicamente verificati e aggiornati, che assicurino coerenza di comportamento all'interno dell'intera struttura aziendale e la tracciabilità delle verifiche svolte e delle valutazioni effettuate in materia di contrasto al riciclaggio e al finanziamento del terrorismo;

- istituzione di adeguati, completi e tempestivi, "flussi informativi" che consentano il monitoraggio delle attività e dei rischi AML-CTF da riportare alla Funzione Antiriciclaggio e da questa verso il Consiglio di Amministrazione per una pronta attuazione delle misure correttive che tenga in considerazione anche le strutture di controllo ed operative, il Gruppo e il Territorio;

- adozione di procedure per la segnalazione al proprio interno di "sistemi di allerta etico" azionabili da parte di dipendenti o di persone in posizione comparabile di violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo (*whistleblowing*);
- diffusione della cultura in materia di antiriciclaggio e di contrasto del finanziamento del terrorismo al fine di sensibilizzare e responsabilizzare tutti i soggetti coinvolti nella gestione del presidio;
- predisposizione, in raccordo con le altre funzioni aziendali competenti in materia di formazione, di un adeguato piano formativo finalizzato a conseguire il continuo aggiornamento del personale e dei collaboratori.

3.2 Assetti organizzativi e flussi informativi

Il modello organizzativo per la gestione del rischio di riciclaggio e finanziamento del terrorismo della Compagnia prevede il coinvolgimento delle seguenti figure aziendali, che, per lo svolgimento delle proprie attività, devono scambiarsi flussi informativi adeguati, completi e tempestivi:

- il Consiglio di Amministrazione, acquisiti i dati, le informazioni sui rischi e sui piani di azione e/o intervento da parte del Responsabile della Funzione Antiriciclaggio, determina le regole, i principi e la linea strategica di contrasto al rischio AML/CTF;
- l'Organo con funzione di gestione (l'Amministratore Delegato della Compagnia) cura l'esecuzione delle misure deliberate e la loro attuazione nella Compagnia, con i compiti identificati nell'art. 11 del Regolamento ed, espressamente, ricomprendendo: (i) l'adozione degli interventi necessari ad assicurare l'efficacia nel tempo dell'organizzazione e del sistema dei controlli antiriciclaggio; (ii) la designazione dei singoli dirigenti, responsabili per l'implementazione di tali controlli; (iii) la formalizzazione delle motivazioni della decisione di non accogliere eventuali proposte di interventi presentate dal responsabile della funzione AML;
- la Funzione Antiriciclaggio, il cui Responsabile (e relativo sostituto nei casi di temporaneo impedimento) svolge altresì il ruolo di Delegato per le segnalazioni delle operazioni sospette;
- le funzioni aziendali di controllo che si devono raccordare con la Funzione Antiriciclaggio;
- i Comitati consiliari, interfunzionali e il comitato esecutivo aziendale (Comex);
- ogni singola unità organizzativa che sia coinvolta in processi antiriciclaggio e di contrasto al finanziamento del terrorismo;
- la "Rete distributiva diretta";

e per ogni utile e/o efficace raccordo a livello di Gruppo

- Comitati e riunioni periodiche di coordinamento con Head Office;
- i Comitati congiunti con funzioni compliance di altre società del Gruppo;
- l'Italy Compliance Committee di Territorio.

3.2.1 Organi sociali e Organo con funzione di gestione

Il Consiglio di Amministrazione e l'Organo con funzione di gestione (l'Amministratore Delegato in conformità al Regolamento n. 44/2019), ciascuno secondo le proprie competenze e responsabilità, previamente acquisite le informazioni, valutazioni e le richieste da parte della Funzione Antiriciclaggio, definiscono e monitorano l'attuazione

delle politiche aziendali e di tutte le necessarie misure organizzative ed operative idonee a gestire il rischio di riciclaggio, ovvero ne controllano il perseguimento (cfr. il Collegio Sindacale).

Specifica cura è rivolta all'adozione di idonei controlli afferenti al rispetto della normativa antiriciclaggio e all'adeguato presidio di tale rischio, anche avvalendosi delle specifiche funzioni e organi di controllo previsti nell'ambito del sistema dei controlli interni.

In tale contesto, l'Organo con funzione di gestione provvederà alla designazione dei dirigenti specificamente delegati alla realizzazione degli interventi, deliberati nel piano di azione che siano ritenuti rilevanti in ambito AML e CTF, al fine di poter assegnare una "prossimità" di competenze, monitoraggio ed esecuzione idonea a consentire una operatività sempre conforme alle leggi e ai Regolamenti.

Il completamento dei presidi e l'efficace svolgimento delle verifiche e la corretta interazione tra funzioni di controllo sarà monitorato anche dall'Organismo di Vigilanza ai sensi dell'articolo 6 del D. Lgs. 231/2001, con specifico riferimento al presidio del rischio di commissione dei reati di riciclaggio, impiego di denaro, beni o utilità di provenienza illecita, anche nella forma del reato di autoriciclaggio, oltre che dei reati di finanziamento del terrorismo e di eversione dell'Ordinamento democratico. L'Organismo di Vigilanza, quale espressione e a diretto riporto del Consiglio di Amministrazione, provvederà a raccordarsi nell'ambito dei compiti di verifica, analisi, valutazione e suggerimento, con la Funzione Antiriciclaggio, quindi, con l'Organo con funzione di gestione per l'esecuzione delle attività.

3.2.2 Comitato per il controllo interno e i rischi (CCIR), Comitato di Sicurezza Finanziaria, Comitato antiriciclaggio, comitato esecutivo aziendale (COMEX) e Comitato Accettazione Clienti (CAC)/KYC Review

Il Comitato per il controllo interno e i rischi, quale Comitato consiliare, assiste il Consiglio di Amministrazione di Cardif Vita S.p.A. con funzione consultiva e propositiva nei seguenti ambiti:

- nella determinazione delle linee di indirizzo del sistema di controllo interno e gestione dei rischi;
- nella verifica periodica dell'adeguatezza e dell'effettivo funzionamento del sistema di controllo interno e gestione dei rischi;
- nell'identificazione e gestione dei principali rischi aziendali, compresi quelli antiriciclaggio.

A livello di applicazione operativa delle misure di contrasto, rilevano:

(I) il "Comitato di Sicurezza Finanziaria", quale Comitato con carattere inter-funzionale presieduto dal Responsabile della Funzione Antiriciclaggio, principalmente, ha lo scopo di:

- (in linea generale e di indirizzo) valutare gli impatti delle novità normative locali e di Gruppo e definire le conseguenti attività progettuali della Compagnia, generate dallo sviluppo del *business* o dalle variazioni normative stesse.

  In tale ambito, si sottolinea, per quanto di competenza ai fini antiriciclaggio, la supervisione costante delle attività aziendali poste in essere per la conformità alle disposizioni previste dalle normative fiscali internazionali (i.e. FATCA ed AEOI), quale attività rilevante attesa la componente fiscale nell'ambito del riciclaggio di capitali e delle questioni di rilevanza (ad es. DAC-6 *reportable transactions*), gestendo la congruità segnaletica oltre che la corretta risoluzione delle criticità e/o delle problematiche;

- (sotto un profilo operativo) analizzare sotto tutti i profili possibili le anomalie e le criticità riscontrate durante l'attività condotta dalla Funzione Antiriciclaggio, anche rivenienti da attività di controllo di "II livello" con riferimento a tutte le tematiche rientranti nella propria area di competenza esclusiva e nel più ampio contesto

esteso alla "*financial security*" (Antiriciclaggio - Antiterrorismo, Sanzioni finanziarie ed Embarghi), nonché dalle attività di controllo di "I livello". In tale contesto, si indica l'analisi delle criticità e delle carenze rilevate, la condivisione delle raccomandazioni formulate per la loro rimozione, nonché lo stato e i tempi di implementazione degli interventi migliorativi, qualora non ancora realizzati, inclusa la valutazione di tutti gli elementi di potenziale rischio da contrastare e l'analisi del piano delle azioni correttive da intraprendere, tenuto conto delle carenze riscontrate nelle verifiche precedenti e di eventuali nuovi rischi identificati;

(II) il "Comitato Antiriciclaggio" il quale, presieduto dal Responsabile AML/Delegato per le segnalazioni delle operazioni sospette - salva e impregiudicata l'attività segnaletica e/o di proposizione di istanze per l'astensione dall'operatività dettate dalla valutazione di gravità del rischio individuato e/o dalla necessità di assolvere (cfr. art. 35 D. lgs. N. 231/07) alla segnalazione, oltre che tempestiva, prima del compimento di ogni operazione - analizza le operazioni presentate dalla Funzione Antiriciclaggio in dipendenza di un sospetto di riciclaggio o qualsiasi altra fattispecie che presenti un livello di rischio significativo in termini di riciclaggio dei capitali, finanziamento del terrorismo, mancato rispetto delle sanzioni finanziarie e delibera ogni attività e/o assume ogni determinazione che sia o risulti conseguente alla determinazione del Delegato SOS;

(III) il COMEX, quale comitato esecutivo aziendale composto dal *top management* presieduto dall'Amministratore Delegato (anche quale Organo con funzione di gestione ai fini AML), assicura il coordinamento e la supervisione delle attività operative svolte all'interno della Compagnia incluse le attività antiriciclaggio.

(IV) il Comitato Accettazione Clienti ("CAC") e il KYC Review hanno quale finalità l'assolvimento di misure di "adeguata verifica rafforzata" (sia quelle previste *ex Lege* e/o a livello regolamentare e/o per regole di Gruppo – ad es. Persone Politicamente Esposte – sia anche quelle rivenienti dalla classificazione della clientela) anche in funzione dei criteri di rischio per specifici Clienti; in particolare, la convocazione di un Comitato (i.e. sia esso il CAC o il KYC Review) ha lo scopo di sottoporre alla valutazione e autorizzazione dell'Amministratore Delegato ovvero di altri soggetti da quest'ultimo delegati (alti dirigenti), al Business ed alla Funzione Antiriciclaggio i rapporti commerciali nuovi ed esistenti che presentano maggiori rischi di riciclaggio di denaro, finanziamento del terrorismo, corruzione, evasione fiscale, violazione delle sanzioni o rischi reputazionali. Nell'ambito di tali Comitati, peraltro, gli alti dirigenti che non intendano adeguarsi al parere della Funzione Antiriciclaggio sono tenuti a formalizzare la motivazione e le misure da adottare per mitigare i rischi segnalati nel parere stesso.

3.2.3 Funzione Antiriciclaggio e altre Funzioni aziendali di controllo

La Funzione Antiriciclaggio è autonoma e indipendente in ogni propria attribuzione, compito e/o attività.

Il Responsabile della Funzione Antiriciclaggio risponde direttamente al Consiglio di Amministrazione e si raccorda con l'Organo con funzione di gestione.

L'istituzione della Funzione Antiriciclaggio è avvenuta (e viene costantemente aggiornata nell'attribuzione dei compiti e delle responsabilità) mediante una specifica delibera del Consiglio di Amministrazione che contestualmente, ne ha definito e ne aggiorna – in conformità alla normativa - i compiti, responsabilità, modalità operative, natura e frequenza della reportistica, nonché l'assegnazione di idonee risorse.

Ai fini organizzativi, attesa la cd. "trasversalità" di impatto degli adempimenti antiriciclaggio, e la stessa interazione che la normativa antiriciclaggio e a contrasto del finanziamento del terrorismo ha con altre materie, la Funzione stessa risulta integrata nella più ampia struttura organizzativa di Compliance.

Tale determinazione è avvenuta al fine di garantire anche a livello organizzativo quanto è già codificato nelle attribuzioni e competenze, prevede al proprio interno una specifica struttura di "KYC & Alert Management" deputata a prevenire e contrastare la realizzazione di operazioni di riciclaggio e di finanziamento del terrorismo, alla quale si affianca la struttura "Control & Reporting" la quale è assegnataria delle attività di controllo di secondo livello, definizione dei flussi di raccolta e conservazione dei dati, nonché attività legate alla strutturazione del *framework* procedurale in materia.

Nell'ambito di Financial Security sono anche svolte attività legate alla fiscalità internazionale (normative FATCA & AEoI) e all'osservanza degli obblighi impeditivi quale è l'osservanza delle sanzioni internazionali/embarghi in considerazione della possibile sovrapposizione dei perimetri.

In tale contesto organizzativo e per dette ragioni, il Responsabile della Funzione Antiriciclaggio è mantenuto coincidente con il Responsabile della Funzione Compliance, proprio nell'ottica e con la finalità di poter agevolare ogni utile individuazione delle normative e valutazione del livello di conformità raggiunta nell'applicazione delle disposizioni e/o regole e/o principi di Gruppo e/o normative locali, nonché al fine di meglio gestire tutte quelle attività aventi carattere trasversale in modo sinergico.

In particolare, la Funzione Antiriciclaggio è munita e deve mantenere la necessaria indipendenza, autonomia funzionale e operativa nonché obiettività di giudizio, di risorse umane, finanziarie e tecnologiche proporzionate alla natura, portata e complessità del business della Compagnia, al fine di raggiungere i complessi obiettivi sopra descritti. Con riferimento alle risorse umane e professionali assegnate alla Funzione, è previsto che queste ultime siano provviste di adeguata professionalità e competenza, pertanto, siano sottoposte ad un costante aggiornamento professionale.

Alla Funzione Antiriciclaggio è garantito libero accesso alle attività dell'impresa, alle strutture aziendali e a tutte le informazioni pertinenti, incluse le informazioni utili a verificare l'adeguatezza dei controlli svolti sulle funzioni esternalizzate.

La Funzione Antiriciclaggio collabora con le altre funzioni aziendali, nonché con gli Organi o le funzioni cui sono assegnati compiti e funzioni di controllo, allo scopo di sviluppare le proprie metodologie di gestione del rischio in modo coerente con le strategie e l'operatività aziendale, disegnando processi conformi alla normativa e prestando attività di consulenza, anche in merito a nuovi prodotti o alla modifica di quelli esistenti.

La Funzione Antiriciclaggio riferisce direttamente, con definita periodicità, al Consiglio di Amministrazione, al Collegio Sindacale e all'Organismo di Vigilanza 231/2001 sull'attività svolta, sulle verifiche effettuate e sulle eventuali raccomandazioni formulate; inoltre, la Funzione informa il Consiglio di Amministrazione, nei casi in cui si renda necessario, previo raccordo con l'Organo con funzione di gestione ed, eventualmente, con le altre Funzioni di controllo, circa le attività svolte, i risultati dei controlli, i rischi individuati ed i fattori di mitigazione e/o le attività correttive predisposti/pianificati/suggeriti, anche attraverso la partecipazione ai comitati aziendali di cui è membro permanente o periodicamente invitato.

3.2.4 Responsabile della Funzione Antiriciclaggio e Responsabile/ Delegato per le segnalazioni delle operazioni sospette

Il Consiglio di Amministrazione provvede alla nomina del Responsabile della Funzione Antiriciclaggio, deputato a svolgere ogni pertinente attività in materia di antiriciclaggio e contrasto al finanziamento del terrorismo.

L'Organo Amministrativo, previamente verificati i requisiti e le competenze necessarie, nonché la necessaria assenza di qualsivoglia compito operativo, sentito l'organo di controllo, provvede al conferimento della delega del "Responsabile per le segnalazioni delle operazioni sospette", che altrimenti sarebbe individuabile *ex Lege* in capo al legale rappresentante della Compagnia.

Il Consiglio di Amministrazione ha nominato il Responsabile della Funzione Antiriciclaggio facendo coincidere il medesimo con il Responsabile della Funzione Compliance.

Il Responsabile della Funzione Antiriciclaggio assiste alle riunioni dell'Organo amministrativo o di quello di controllo, su richiesta del rispettivo Presidente. La partecipazione può essere prevista anche in via stabile, in relazione alle materie trattate.

Il Responsabile/ Delegato per le segnalazioni delle operazioni sospette ("Delegato SOS") si identifica nel Responsabile della Funzione Antiriciclaggio, sulla base di apposita nomina da parte del Consiglio di Amministrazione.

Il Delegato SOS ha il principale compito di esaminare e trasmettere alla UIF le segnalazioni delle operazioni sospette ritenute fondate, attribuendo una valutazione di rischio coerente con le risultanze delle motivazioni addotte, nonché determinando gli effetti sia sulla classificazione di rischio sia anche sull'eventuale opportunità nell'adozione di misure conseguenti al rischio (ad es. proposta di risoluzione di rapporto e/o astensione e/o monitoraggio dei flussi monetari). Ha libero accesso ai flussi informativi diretti agli organi aziendali ed alle strutture coinvolte nella gestione e nel contrasto del rischio di riciclaggio. Ha il compito di intrattenere i rapporti con la UIF e di rispondere tempestivamente ad eventuali richieste formulate dalla stessa Unità. Il predetto Delegato ha, inoltre, il compito di effettuare ogni utile allineamento informativo e adeguamento della valutazione di rischio con il Responsabile della Funzione Antiriciclaggio, ragione per la quale la scelta di farli coincidere è ritenuta conforme alla normativa e coerente con l'impostazione di un adeguato sistema di controlli.

L'assunzione della carica di Responsabile della Funzione Antiriciclaggio e di Delegato SOS è vincolata al possesso di specifici requisiti di professionalità, onorabilità e indipendenza (cfr. articolo 15, comma 2 e art. 18 comma 3 del Regolamento IVASS n. 44, anche in linea con quanto previsto dal Decreto Ministeriale del 02/05/2022 n. 88[10]).

In particolare, è previsto:

- per il requisito di professionalità - il possesso di almeno n. 5 anni di esperienza nell'esercizio di una o più delle seguenti attività:
  - attività nella Funzione Antiriciclaggio, Compliance, di Revisione Interna, Legale o Risk Management presso società ed enti del settore assicurativo, creditizio o finanziario;
  - attività nella Funzione Compliance, di Revisione Interna, Legale o Risk Management in imprese pubbliche e private aventi dimensioni adeguate a quelle di Cardif Vita S.p.A.;
  - attività professionali e/o consulenziali e/o di controllo attinenti alle attività di antiriciclaggio, compliance, revisione interna, legale o risk management nel settore assicurativo, creditizio o finanziario, o attività di insegnamento universitario di ruolo in materie giuridiche o economiche aventi rilievo per la Funzione Antiriciclaggio (inclusa ogni attività di interazione con le Autorità di Vigilanza);
  - attività svolta quale dipendente di Autorità di Vigilanza o Controllo in materia di prevenzione e contrasto al riciclaggio e finanziamento del terrorismo ovvero di Autorità di Polizia con compiti in tali materie.
- Per il requisito di onorabilità l'assenza delle seguenti cause ostative all'esercizio dell'incarico:
  - stato di interdizione legale ovvero interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese e, comunque, tutte le situazioni previste dall'articolo 2382 del Codice Civile;
  - sottoposizione a misure di prevenzione disposte dall'autorità giudiziaria ai sensi della legge n. 1423/56 o della legge n. 575/65 e della legge n. 646/82, e successive modificazioni ed integrazioni, salvi gli effetti della riabilitazione;
  - stato di condannato con sentenza definitiva (salvi gli effetti della riabilitazione):
    1) a pena detentiva per uno dei reati previsti dalla normativa speciale che regola il settore assicurativo, bancario, finanziario, dei valori mobiliari e dei mercati e degli strumenti finanziari nonché previsti dal D. Lgs. 231/2007 e successive modificazioni ed integrazioni;
    2) alla reclusione per uno dei delitti previsti nel titolo XI del libro V del Codice Civile ("Disposizioni penali in materia di società e consorzi") e nel Regio Decreto n. 267/42 ("Disciplina del fallimento, del concordato preventivo, dell'amministrazione controllata e della liquidazione coatta amministrativa");
    3) alla reclusione per un tempo non inferiore ad un anno per un delitto contro la pubblica amministrazione, contro la fede pubblica, contro il patrimonio, contro l'ordine pubblico, contro l'economia pubblica ovvero per un delitto in materia tributaria;
    4) alla reclusione per un tempo non inferiore a due anni per un qualunque delitto non colposo.
- Per i requisiti di autonomia e indipendenza è richiesto, inoltre, che i soggetti:
  - non siano a capo di aree operative, né gerarchicamente dipendenti dai soggetti responsabili di dette aree;
  - dispongano di risorse umane, in possesso di conoscenze specialistiche e di cui è curato l'aggiornamento professionale, tecnologiche e finanziarie adeguate allo svolgimento dell'attività;
  - abbiano libero accesso alle attività dell'impresa, alle strutture aziendali e a tutte le informazioni pertinenti, incluse le informazioni utili a verificare l'adeguatezza dei controlli svolti sulle funzioni esternalizzate;
  - riferiscano direttamente all'organo amministrativo a cui, mediante adeguate procedure di reporting, danno contezza dell'attività svolta, dei risultati delle verifiche effettuate e rivolgono eventuali raccomandazioni.

[10] Regolamento in materia di requisiti e criteri di idoneità allo svolgimento dell'incarico degli esponenti aziendali e di coloro che svolgono funzioni fondamentali ai sensi dell'articolo 76, del codice delle assicurazioni, di cui al decreto legislativo 7 settembre 2005, n. 209.

In tale contesto, i candidati alla posizione di responsabile e personale più elevato delle funzioni fondamentali (Risk Management, Actuarial Function, Compliance, Internal Audit) vengono proposti al Consiglio di Amministrazione dall'Amministratore Delegato. Laddove dette funzioni fondamentali siano "integrate" nel Gruppo BNP Paribas Cardif (Risk Management, Compliance, Internal Audit), l'Amministratore Delegato dovrà ottenere un parere preventivo dai Responsabili, non vincolante, delle funzioni fondamentali a livello di Gruppo.

Il requisito di indipendenza "organizzativa" è garantito dall'inclusione della Funzione Antiriciclaggio e del Delegato SOS all'interno della Funzione fondamentale Compliance e del riconoscimento della vincolatività del parere espresso da detti soggetti sulle tematiche afferenti al Regolamento IVASS 44/2019.

La valutazione di sussistenza dei requisiti di professionalità, onorabilità autonomia e indipendenza dei soggetti interessati è effettuata da parte del Consiglio di Amministrazione, almeno una volta l'anno, previa acquisizione delle evidenze a supporto della valutazione come specificate presente Politica.

In aggiunta alle valutazioni effettuate a seguito di nuove assunzioni ed alla valutazione periodica dei requisiti, nel caso in cui emerga la possibilità che i soggetti interessati non garantiscano più la conformità con i requisiti del ruolo esercitato, il Consiglio di Amministrazione effettua una nuova valutazione. In particolare, tale verifica deve essere eseguita ogniqualvolta sussistano ragioni per ritenere che il soggetto interessato possa:

- indurre l'impresa ad agire in contrasto con la normativa vigente;
- aumentare il rischio che siano commessi reati finanziari;
- mettere in pericolo la sana e prudente gestione dell'impresa.

Relativamente al Responsabile della Funzione antiriciclaggio, l'impresa comunica all'IVASS, tempestivamente e comunque non oltre trenta giorni dall'adozione del relativo atto o dal verificarsi della relativa fattispecie, il conferimento dell'incarico, il rinnovo e le eventuali dimissioni, decadenza, sospensione e revoca, nonché ogni elemento sopravvenuto che possa incidere sulla valutazione dell'idoneità alla carica. L'obbligo ricorre anche in caso di esternalizzazione o sub-esternalizzazione della Funzione antiriciclaggio.

Oltre alla comunicazione di cui al precedente paragrafo, le valutazioni dell'Organo Amministrativo in merito al possesso dei requisiti sono comunicate all'IVASS, entro n. 30 giorni dall'adozione, mediante la trasmissione della relativa delibera adeguatamente motivata. Nel caso di nomina o rinnovo, l'impresa attesta di aver effettuato le verifiche sulla sussistenza dei requisiti, fornendo adeguata motivazione in merito alla valutazione effettuata. La delibera riporta analiticamente i presupposti su cui l'impresa ha svolto la valutazione e le relative conclusioni cui è pervenuta. L'IVASS si riserva la facoltà, ove lo ritenga opportuno, di richiedere all'impresa l'acquisizione della documentazione analizzata a supporto della valutazione

La comunicazione dei predetti dati, secondo le istruzioni tecniche fornite dall'IVASS, rese disponibili sul sito dell'Istituto, è effettuata dal Responsabile della Funzione Legal & Corporate Affairs che altresì garantisce la centralizzazione e l'archiviazione dei file di notifica.

Con riferimento specifico al Responsabile per le segnalazioni delle operazioni sospette di cui all'art. 18 del Regolamento 44, le sue generalità sono tempestivamente comunicate all'UIF, con le modalità dalla stessa stabilite: alla medesima autorità viene altresì comunicata ogni successiva variazione, sostituzione e/o delega.

3.2.5 Unità organizzative aziendali

Specifiche unità organizzative aziendali sono chiamate a svolgere attività connesse alla gestione del rischio di riciclaggio e contrasto al finanziamento del terrorismo. Si riportano, di seguito, per ciascuna Direzione aziendale coinvolta, le principali aree in cui si inseriscono le attività di carattere operativo svolte, riconducibili ai processi antiriciclaggio che richiedono il coinvolgimento della Funzione antiriciclaggio per la valutazione/ gestione degli aspetti di competenza.

- Organo con funzione di gestione, in ambito antiriciclaggio si intende l'Amministratore Delegato deputato al monitoraggio dell'esecuzione delle deliberazioni assunte dal Consiglio di Amministrazione in materia AML e

CTF, altresì, assegnatario dei compiti di (i) designazione dei singoli dirigenti, appartenenti all'Alta Direzione, specificamente delegati alla realizzazione di ciascun intervento e per il monitoraggio di quanto da essi realizzato; (ii) formalizzazione, con adeguate motivazioni, della decisione di non accogliere eventuali proposte di interventi organizzativi e procedurali presentate dal responsabile della funzione antiriciclaggio; (iii) dell'esecuzione e/o modifica – tempo per tempo – delle attività AML e CTF – al fine di tenere conto degli orientamenti e delle indicazioni emanate dalle autorità.

- La Funzione Antiriciclaggio della Compagnia è inserita nella struttura organizzativa di Compliance, che riporta al Consiglio di Amministrazione della Compagnia. Il Responsabile della Funzione Compliance è anche il Responsabile della Funzione Antiriciclaggio della Compagnia nonché Delegato per la segnalazione delle operazioni sospette. La Funzione Antiriciclaggio beneficia, inoltre, del supporto delle altre strutture di Compliance. In primo luogo del team "Compliance Operating & Regulatory Office" che svolge prevalentemente attività legate all'analisi ed alla valutazione unitaria del rischio di non conformità, ricomprendendo nello stesso anche quello derivante dalla possibile violazione degli obblighi previsti dalla normativa antiriciclaggio e di contrasto del finanziamento del terrorismo che possiedono indubbi elementi di "trasversalità" (ad es. interazioni con normativa anticorruzione e/o, in generale, conformità normativa a Leggi e/o regolamenti). Detto team è inoltre responsabile della pianificazione delle attività, della raccolta dei fabbisogni formativi e della finalizzazione della rendicontazione verso gli Organi Societari, l'Organo con funzione di gestione ed Head Office. Al suo interno è inoltre collocata la figura del CCRM che ha tra le sue responsabilità quella di effettuare controlli di secondo livello ("GCP - Generic Control Plan"), anche su alcune attività di antiriciclaggio conformemente alle procedure di Gruppo. Importanti sinergie sono poi sviluppate con il team "Protection of Interest of Clients & Professional Ethics", per garantire una visione unitaria in materia di prodotti ed intermediari.

- Customer Service è la struttura volta a presidiare i processi operativi connessi alla gestione tecnica del portafoglio nonché quelli relativi alla liquidazione delle polizze, avendo come finalità l'erogazione di un servizio di qualità al cliente, nel rispetto dei regolamenti e delle procedure interne ed esterne, degli obiettivi definiti dall'azienda, congiuntamente ad un costante controllo dei rischi operativi, finanziari e normativi. Le attività del Customer Service consistono, tra le altre, nel presidiare le attività operative connesse agli adempimenti regolamentari in materia di sicurezza finanziaria.
    - Regulatory Controls è l'unità di Operations Controls, all'interno della struttura Customer Service, che opera all'interno della prima linea di difesa e contribuisce a garantire la divisione tra i controlli di primo e secondo livello sul corretto adempimento degli obblighi AML/ CTF. In particolare: gestisce il processo per l'analisi di *due diligence* dei clienti; cura e gestisce l'organizzazione e la tenuta del Comitato di Accettazione Clienti ("CAC") e del KYC Review; monitora ed analizza le operazioni potenzialmente sospette; garantisce l'affidabilità e la corretta alimentazione dell'AUI; monitora e gestisce il Registro dei PEPs; gestisce le richieste di autorizzazione preventiva avanzate dalla rete o dagli uffici interni della Compagnia e sottopone all'attenzione della Funzione Antiriciclaggio le anomalie significative rilevate.

- Process Engineering, cura lo sviluppo e l'implementazione di metodologie e di strumenti per il disegno / revisione dei processi, supportando tutte le funzioni aziendali. Si occupa inoltre, con riferimento alle iniziative di principale interesse per l'azienda del disegno/ revisione dei processi in ottica end to end, al fine di: massimizzare l'efficienza e l'efficacia; presidiare i rischi operativi, assicurando anche la definizione dei punti di controllo di primo livello e/o gerarchici; definire e monitorare gli SLA di processo.

- Human Resources, si occupa di (i) integrare nel più generale Piano di formazione aziendale, le attività formative definite dalla Funzione Antiriciclaggio sui temi di propria competenza, nonché del monitoraggio del piano formativo rivolto al personale e ai collaboratori, (ii) di garantire, in collaborazione con Process Engineering, il corretto dimensionamento delle unità organizzative, nonché (iii) di effettuare il controllo in fase di assunzione ex art. 19 del CCNL delle Imprese di assicurazione.

- Operational Permanent Control (OPC), (i) garantisce la rilevazione, la valutazione e la verifica di tutte le segnalazioni di incidente operativo; (ii) supporta e controlla l'attuazione dei piani d'azione definiti dai Responsabili locali al fine di ridurre al minimo il livello di rischio e di eliminare o ridurre le conseguenze degli incidenti operativi; (iii) garantisce l'applicazione del piano dei controlli richiesto dal Gruppo per la mitigazione del rischio operativo e del rischio di conformità, inserendo eventuali controlli specifici per la mitigazione dei rischi locali; (iv) garantisce l'esecuzione, su base annuale, del Piano dei Controlli Permanenti (OPC Control Plan) richiesto dal Gruppo, integrabile nel corso dell'anno a seguito di specifiche esigenze aziendali, risultanti dalle principali evidenze di rischio operativo, ed esegue i relativi test; (v) gestisce e

garantisce l'aggiornamento della Mappatura dei Rischi Operativi della Compagnia e dei rischi di conformità secondo la metodologia di HO (RCSA – Risk & Control Self Assessment); (vi) supporta i Responsabili della Compagnia nel monitoraggio delle attività in *outsourcing* ai sensi del Reg. 38 IVASS e controlla l'applicazione dei relativi piani di azione; (vii) gestisce il follow-up delle raccomandazioni e dei findings emessi dalla Revisione Interna dai Revisori Esterni e dalla funzione Risk di Gruppo ad eccezione di quelle direttamente a carico della Funzione Compliance.

  - Distribution Controls, nell'ambito della struttura di OPC, predispone la reportistica necessaria all'accreditamento ed alla valutazione degli Intermediari / Partner, secondo quanto previsto dalle procedure aziendali (KYI / KYC). Effettua inoltre la revisione periodica delle controparti stesse.

- Governance Management, assicura la completezza dell'impianto normativo interno ed il progressivo aggiornamento anche in linea con le indicazioni del Regolatore locale nonché con le indicazioni di Gruppo; supporta il General Secretary nel sovrintendere la *governance* della Compagnia al fine di migliorare il processo decisionale basato sulla revisione periodica dei Comitati aziendali; Garantisce, nel ruolo di Head of Conduct, il recepimento della normativa legislativa e regolamentare di rilevanza per l'attività aziendale riportando in questo ruolo al coordinatore di Head Office; mantiene aggiornato e strutturato il *repository* delle procedure al fine di garantire a tutte le Funzioni l'efficace consultazione delle stesse.

  - Regulatory Programs, nell'ambito della Funzione di Governance Management che si occupa del governo complessivo dei programmi regolamentari di maggior rilevanza per la Compagnia promuovendo l'adozione dei modelli di governo efficaci e collegiali in rapporto alle richieste degli *stakeholders* della Compagnia (HO, Regulators, Organo Amministrativo, etc.) preservando al contempo le specificità locali della Compagnia.

  - Local Conduct Referent, inserito nell'ambito della struttura di Governance, ha quale obiettivo quello di assicurare l'integrazione delle regole e raccomandazioni previste dal Codice di Condotta all'interno dei processi operativi, ivi inclusi quelli ricompresi alle tematiche relative al riciclaggio ed al finanziamento del terrorismo.

- Data Office, supporta la Funzione Compliance, nonché la Funzione Antiriciclaggio (ad oggi incorporata nella Funzione Compliance), nella valutazione periodica e nel conseguimento della conformità alle normative interne ed esterne con impatti diretti sulla Data Governance e sulla qualità dei dati, anche attraverso controlli dedicati, analizzando gli impatti ed identificando e coordinando gli interventi di adeguamento o le azioni correttive individuate nello svolgimento delle attività di competenza.

3.2.6 Rete distributiva

La Compagnia si avvale nella distribuzione di prodotti assicurativi di una rete distributiva principalmente tramite un modello di distribuzione definito B to B to C[11]. Ne consegue la necessità di adottare ogni precauzione volta ad assicurare il rispetto delle disposizioni in materia di contrasto al riciclaggio ed al finanziamento del terrorismo.

La Compagnia introduce opportuni meccanismi volti alla valutazione della qualità degli intermediari in relazione all'affidabilità degli stessi, anche da un punto di vista dell'assolvimento degli obblighi antiriciclaggio-antiterrorismo ed anche quale Intermediario qualificato che possa svolgere le attività di adeguata verifica nei confronti della Clientela, per conto della Compagnia stessa.

Nei confronti della rete distributiva intermediata vengono effettuate delle preventive analisi di *due diligence* che vengono aggiornate nel corso e quale condizione per il mantenimento della relazione con la Compagnia.

In particolare, è previsto:

[11] Sebbene in via residuale e al presentarsi di specifiche situazioni, Cardif Vita S.p.A. può ricorrere anche all'apertura e alla gestione diretta del rapporto assicurativo e delle operazioni per i dipendenti e per la clientela cd disintermediata. Cfr: Procedura CAN 03-02-01 KYC & Due Diligence per la Clientela Diretta Interna.

- un processo di Know Your Intermediary ("KYI"), da agire nei confronti degli intermediari attivi per i rapporti in essere o nei confronti di potenziali intermediari, che si conforma, oltre che al principio di "adeguata verifica semplificata", ai principi delle Linee Guida EBA-ESMA ed EIOPA e, sotto il profilo operativo e di rispetto delle disposizioni antiriciclaggio, a quelli indicati dal Wolfsberg Group, che deve essere applicato quale condizione preventiva rispetto all'accettazione dell'intermediario e antecedentemente rispetto all'avvio di una nuova relazione di business con quest'ultimo, o quale condizione per confermare il mantenimento della relazione per quelle già esistenti, e ha l'obiettivo di:
    - conoscere l'identità, la natura del business e la tipologia di clientela del soggetto che distribuirà il prodotto della Compagnia;
    - verificare, ove necessario, che l'intermediario sia dotato di adeguati presidi antiriciclaggio e di contrasto del finanziamento del terrorismo;
    - controllare che l'intermediario ed i propri *stakeholders* non risultino presenti nelle "liste di sorveglianza";
    - verificare la presenza di eventuali rischi reputazionali per Cardif, nonché per il Gruppo BNP Paribas, in base alle informazioni rinvenute dalle fonti pubbliche disponibili;
    - controllare l'eventuale presenza di conflitti di interesse tra la Compagnia e l'intermediario ovvero tra l'intermediario ed i dipendenti della Compagnia (es: un intermediario è anche un dipendente/collaboratore del Gruppo BNP Paribas Cardif, oppure un dipendente/collaboratore di Cardif è azionista del potenziale intermediario);
    - monitorare attivamente e costantemente, nel corso della relazione, qualsiasi evento o informazione che possa costituire un rischio per la Compagnia.
- un processo specifico di "*due diligence*" dal punto di vista antiriciclaggio e di contrasto del finanziamento del terrorismo, che prevede l'acquisizione per iscritto di ogni dato, informazione e/o documento utile ad attestare la conformità alle risultanze sopra indicate.

  Per quanto concerne le "attività delegate" da Cardif Vita a Banca BNL, principale intermediario della Compagnia, nel Service Level Agreement stipulato dalle parti è rappresentata la descrizione del dettaglio operativo e delle tempistiche di attuazione degli "Adempimenti Antiriciclaggio, Contrasto al Finanziamento del Terrorismo, Rispetto degli Embarghi e Sanzioni Finanziarie Internazionali e Anticorruzione". Pertanto, ferma la responsabilità della Compagnia nell'assolvimento di tali adempimenti, è prevista la "codificazione" del dettaglio degli obblighi in apposite clausole contrattuali, l'effettuazione di verifiche (tramite inclusione di specifici diritti di *audit*) da parte della Compagnia ed anche il diritto di accesso e/o la risoluzione automatica al verificarsi di determinati eventi che costituiscano condizione di improcedibilità nella relazione e/o l'esistenza di un elevato rischio in materia di antiriciclaggio e antiterrorismo.

Anche negli altri accordi di distribuzione sono chiaramente definiti gli adempimenti di "adeguata verifica" delegati dalla Compagnia agli intermediari stessi, nonché l'obbligo di esercizio dell'astensione dall'operatività nei casi previsti dalla normativa antiriciclaggio-antiterrorismo.

Inoltre, nell'ambito di dette clausole, è previsto quanto segue:

- predisposizione di ogni idonea misura che consenta una adeguata implementazione dei sistemi informativi per la gestione degli adempimenti a svolgersi per conto delle Compagnie,
- adeguata e regolare formazione in materia di antiriciclaggio/antiterrorismo da parte dell'intermediario del proprio personale;
- comunicazione da parte dell'intermediario alle Compagnie e viceversa dell'avvio di eventuali approfondimenti inerenti a clienti comuni e/o riferiti alle medesime operazioni, pur rimanendo distinta la competenza tra intermediario e Compagnia in relazione all'eventuale decisione di provvedere alla segnalazione di operazioni sospette.

È altresì disposto che nei **contratti/ accordi di collaborazione** con gli intermediari costituenti la rete distributiva siano specificate le **regole di comportamento vincolanti anche per la segnalazione di operazioni sospette** a fini del contrasto al riciclaggio ed al finanziamento del terrorismo cui gli stessi devono attenersi nell'esercizio della propria attività

Da ultimo si segnala che in sede di controlli annuali sulla qualità della vendita svolti da OPC (Operational Permanent Controls) viene raccolta, un'autocertificazione dal distributore attestante, tra l'altro, l'adempimento degli obblighi previsti dalla normativa antiriciclaggio.

3.2.7 Flussi informativi

Devono essere assicurati flussi informativi idonei e canali di comunicazione adeguati a presidiare il rischio di riciclaggio in conformità con le disposizioni sul sistema di governo societario (cfr. articolo 8 e articolo 10, comma 1, lettera f) del Regolamento IVASS n. 44).

Nello specifico, al fine di garantire la piena valorizzazione dei diversi livelli di responsabilità all'interno dell'organizzazione aziendale, la Compagnia assicura la presenza di flussi informativi adeguati, completi e tempestivi verso gli organi sociali (tra cui Consiglio di Amministrazione e Organo con funzione di gestione) e tra la Funzione Antiriciclaggio e le funzioni fondamentali interessate dalla tematica, nonché con ogni altro organo o funzione deputati al controllo, con le strutture organizzative, la rete distributiva, Head Office e il Territorio.

Inoltre, in tema di flussi informativi assume rilevanza anche l'eventuale condivisione delle informazioni con altre entità del Gruppo, come riconosciuto dalla normativa interna[12].

I principi ivi espressi postulano che le informazioni in ambito AML/CTF relative alla clientela ed alle transazioni siano condivise in ottemperanza alla regolamentazione internazionale, comunitaria e locale.

Lo scambio informativo tra diverse società del Gruppo relativamente alla clientela comune contribuisce in maniera significativa a rafforzare i presidi a contrasto del riciclaggio e del finanziamento del terrorismo pur dovendosi tenere in considerazione l'esigenza di garantire un'adeguata protezione dei dati personali dei clienti. In argomento, la Compagnia promuove nel continuo i predetti principi di condivisione informativa descritti attraverso processi di scambio con i principali partner infragruppo, che hanno l'obiettivo di (i) garantire l'allineamento dei profili di rischio della clientela comune in conformità con i requisiti normativi locali, nonché (ii) ottenere informazioni sempre aggiornate sui clienti comuni.

Più in generale, per quanto concerne i flussi informativi verso la rete distributiva, si segnala, inoltre, che la Compagnia, conformemente a quanto previsto dal Reg. IVASS 44/2019, così come modificato ai sensi dell'art. 10 co. 4 del Provv. IVASS 111/2021, procede annualmente alla comunicazione verso ciascun broker ed agente dei premi lordi contabilizzati. Tale comunicazione viene effettuata tramite posta elettronica certificata entro n. 10 giorni dalla trasmissione dei medesimi dati ad IVASS nell'ambito dell'esercizio di autovalutazione (rif. scadenza 30 giugno di ogni anno).

La Compagnia, infine, adotta procedure per la segnalazione al proprio interno da parte di dipendenti, o di persone in posizione comparabile, di violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo (*whistleblowing*).

Tali procedure garantiscono:

- la tutela della riservatezza dell'identità del segnalante e del presunto responsabile delle violazioni, ferme restando le regole che disciplinano le indagini e i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto delle segnalazioni;
- la tutela del soggetto che effettua la segnalazione contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione;
- lo sviluppo di uno specifico canale di segnalazione, anonimo e indipendente, proporzionato alla natura e alle dimensioni delle imprese;
- l'analisi e la "tracciabilità" di segnalazioni che pervengano anche prive di tutti gli elementi essenziali all'effettuazione di una istruttoria;

[12]Si confronti paragrafo 4.7. della INS-CPL-FS01 v.11 Global AML-CTF Policy

- il contrasto e l'attivazione di procedure di responsabilità, come previste ex lege, in caso di segnalazioni meramente denigratorie e/o lesive di interessi altrui, senza che sia apprezzabile (all'esito delle attività di analisi) alcun reale e/o effettivo intento di segnalazione di condotte costituenti reato.

Ulteriori dettagli circa il processo di *reporting*, per categoria di soggetti, sono contenuti nel "Documento analitico" redatto ai sensi dell'articolo 11, comma 1, lettera c) del Regolamento IVASS n. 44.

3.2.8 Supervisione consolidata di Gruppo

Sul piano generale del sistema dei controlli interni, di significativa importanza sono gli standard internazionali stabiliti all'interno delle Raccomandazioni GAFI[13]. In particolare, secondo la raccomandazione GAFI n. 18 i gruppi finanziari devono garantire l'implementazione presso ciascuna entità di programmi per il contrasto del riciclaggio e del finanziamento del terrorismo.

Tale requisito è soddisfatto da BNP Paribas attraverso:

- procedure omogenee in materia AML/CTF basate sui rischi identificati nell'ambito del ML-TF Risk Classification;
- regole comuni in termini di identificazione e verifica dei rischi di riciclaggio e finanziamento del terrorismo;
- un solido sistema di controllo interno per valutare l'efficienza complessiva del *framework* AML-CTF.

A tal fine, in ossequio a quanto previsto dalla Politica Antiriciclaggio di Gruppo, la Compagnia fornisce a sua volta informazioni sufficientemente precise ed esaustive valide per il monitoraggio consolidato dei rischi di riciclaggio e di contrasto al finanziamento del terrorismo. Le eventuali debolezze individuate sono di conseguenza gestite tramite piani di azione condivisi con le strutture del Gruppo stesso.

3.3 Linee di difesa

Un idoneo sistema di controllo interno che garantisca nel tempo la mitigazione e la gestione dei rischi di riciclaggio e di finanziamento del terrorismo deve essere istituito e manutenuto in ragione delle risultanze delle verifiche attuate, disponendo ogni adeguamento eventualmente necessario (cfr. art. 6 comma 1 del Regolamento IVASS n. 44).

L'Organo con funzione di gestione è responsabile per l'adozione degli interventi necessari ad assicurare l'efficacia nel tempo del sistema dei controlli antiriciclaggio, mentre la Funzione Antiriciclaggio collabora alla sua individuazione e provvede a verificarne nel continuo l'idoneità (cfr. art. 11 comma 1 lettera b) e art. 14 comma 2) lettere d) ed e) del Regolamento IVASS n. 44).

Il sistema di controllo, in particolare, si articola in:

- controlli di linea (I livello);
- controlli assegnati alla Funzione Antiriciclaggio (II livello);
- controlli svolti dalla Funzione di Internal Audit (III livello).

Con riferimento al presidio di I livello, assumono valenza fondamentale i controlli di linea integrati nelle procedure informatiche, che comportano possibili blocchi / sospensive.

[13] Gruppo d'Azione Finanziaria ("GAFI" o anche "FATF", Financial Action Task Force) è un organismo intergovernativo che ha lo scopo di fissare standard internazionali per la lotta al riciclaggio e al finanziamento del terrorismo. È stato fondato nel 1989 ed ha sede a Parigi.

L'unità "Regulatory Controls", inserita nell'ambito della struttura Operations Controls, a riporto della Funzione Customer Service, a supporto della Funzione Antiriciclaggio:

- gestisce il processo per l'analisi di *due diligence* dei clienti sulla base dei criteri stabiliti dalle relative procedure nonché per l'accesso in consultazione e verifica al "registro di titolarità effettiva"[14];
- effettua l'analisi dei *dossier* ad alto rischio da sottoporre all'autorizzazione della Funzione Antiriciclaggio e le attività istruttorie;
- conduce la revisione (con le tempistiche di volta in volta decise in sede di Comitato CAC e KYC Review, nonché sulla base del livello di rischio associabile e conformemente alle procedure di Gruppo applicabili) dei *dossier* relativi ai clienti "sensibili";
- gestisce e cura l'organizzazione del Comitato di Accettazione Clienti e del KYC Review;
- svolge le verifiche circa l'allineamento del *tool* KYC alle decisioni tempo per tempo assunte;
- verifica preliminarmente qualsiasi posizione ad alto rischio di riciclaggio individuata dalla Compagnia o segnalata dalle diverse Autorità;
- analizza gli *alert* delle operazioni potenzialmente sospette generati dalla piattaforma informatica adottata dalla Compagnia e segnala le eventuali anomalie significative alla Funzione Antiriciclaggio contestualmente predisponendo ogni annotazione motivazionale utile alla valutazione e, del caso, archiviazione di quanto esaminato e giustificato;
- analizza gli esiti delle verifiche effettuate attraverso le liste di sorveglianza;
- garantisce l'affidabilità e la corretta alimentazione dell'AUI anche nel caso di, eventuale, operatività transfrontaliera[15];
- monitora e gestisce i criteri di consultazione, accesso e riscontro (anche per le segnalazioni di incongruenze) al "registro dei titolari effettivi"[16] sia sotto un profilo di (a) classi di rischio della clientela; (b) tipologie e classi di rischio dei prodotti; (c) altri fattori di rischio che possano avere influenza anche sui criteri precedentemente indicati;
- monitora e gestisce il Registro dei PEPs;
- gestisce le richieste di autorizzazione preventiva avanzate dalla rete o dagli uffici interni della Compagnia e sottopone all'attenzione della Funzione Antiriciclaggio le anomalie significative rilevate, anche ai fini della contribuzione segnaletica verso il "registro dei titolari effettivi" (e relativi criteri di identificazione).

La Funzione Antiriciclaggio è responsabile dello svolgimento dei controlli di II livello. In particolare, tale funzione, anche attraverso il supporto dei *team* della Funzione Compliance:

- collabora all'individuazione e mantenimento, in termini di efficienza ed efficacia, del sistema di controllo interno finalizzato alla prevenzione del rischio di riciclaggio e all'individuazione e adeguamento delle relative regole di controllo degli strumenti di *detection* e/o di profilazione del rischio AML;
- svolge le attività di controllo previste dal piano annuale;
- effettua i controlli di II Livello sulle attività di I livello dell'unità Regulatory Controls inserita nell'ambito della struttura Operations Controls, nonché sugli altri controlli di I livello eseguiti dalle funzioni operative;
- verifica i criteri di alimentazione utili alla conservazione dei dati ed i criteri di classificazione delle informazioni; verifica, sotto il profilo operativo, l'effettiva applicazione delle procedure antiriciclaggio e antiterrorismo, in particolare "adeguata verifica", "registrazione e conservazione dei dati", "rilevazione, valutazione e

[14] Si precisa che al momento della stesura della Presente Politica risultano ancora in corso di emissione i provvedimenti attuativi del "Registro della Titolarità Effettiva", previsti ai sensi del Decreto nr. 55 del 11 marzo 2022 del Ministero dell'Economia e delle Finanze, pertanto tutte le attività legate al registro della titolarità effettiva sono da considerarsi sospese fino all'entrata in vigore dello stesso.

[15] Effettuata sempre nei limiti dell'autorizzazione all'attività assicurativa.

[16] Da intendersi applicabile dal momento dell'entrata in vigore del provvedimento che ne sancisce l'effettiva operatività.

segnalazione di operazioni sospette", individuandone (eventuali) potenziali criticità, al fine di suggerire le misure correttive;

- effettua attività di controllo periodico (anche cartolare) nei confronti degli Intermediari e degli *outsourcers* ai quali la Compagnia ha conferito delega ad effettuare, l'attuazione degli adempimenti previsti dalla normativa antiriciclaggio;
- aggiorna costantemente il Responsabile della Funzione AML (che ne potrà riportare direttamente e/o chiedere l'invio periodico anche al Comitato di Sicurezza Finanziaria) sui controlli eseguiti, le eventuali anomalie rilevate e i relativi piani di intervento correttivi necessari, curandone la redazione delle verbalizzazioni e delle determinazioni.

Inoltre, la Funzione Antiriciclaggio in materia di adeguata verifica:

- monitora, a seguito di segnalazioni e/o comunicazioni da parte del primo livello, l'operatività dei clienti al fine di individuare eventuali anomalie;
- analizza le posizioni ad alto rischio di riciclaggio individuate dalla prima linea di difesa o segnalate dalle diverse Autorità (in tal caso, considerando anche le richieste di approfondimenti, la notifica di accertamenti), anche tenendo in considerazione eventuali provvedimenti sanzionatori; la conoscenza dell'avvio di indagini (anche fiscali) e/o la conoscenza di altre notizie pregiudizievoli;
- contribuisce ad "evento" e/o in modalità "ricorrente" alla rinnovazione della "adeguata verifica" tramite la revisione periodica dei dossier relativi ai clienti sulla base del livello di rischio agli stessi associabile, anche conformemente alle procedure di Gruppo applicabili.

La Funzione di Internal Audit è responsabile dello svolgimento dei controlli di III livello. In particolare, tale funzione verifica:

- il dispositivo di Governance, Gestione dei Rischi e Controllo Interno in materia di antiriciclaggio;
- il costante rispetto degli obblighi di adeguata verifica dei rapporti continuativi, sia nella fase di instaurazione che nel corso dello svolgimento degli stessi, fino alla loro conclusione;
- l'acquisizione e l'ordinata conservazione dei dati, delle informazioni e dei documenti prescritti dalla normativa;
- il corretto funzionamento degli archivi informatici utilizzati per la conservazione dei dati e delle informazioni;
- la consapevolezza del personale e della rete distributiva diretta in merito alla portata dell'obbligo di collaborazione attiva;

raccordandosi con la Funzione Antiriciclaggio per ogni eventuale, opportuno, necessario e/o utile, intervento di adeguamento.

La Funzione di Internal Audit pianifica e conduce verifiche in materia di rischi di riciclaggio. Tali verifiche interessano sia le strutture operative interne, che l'adeguatezza e le risultanze dei controlli svolti sulla rete distributiva diretta e sulle terze parti a cui siano state esternalizzate attività che interessino il *framework* antiriciclaggio. Inoltre, la Funzione indica gli interventi correttivi da adottare per la rimozione delle criticità riscontrate nell'ambito delle predette verifiche e ne riscontra l'adozione e l'efficacia in sede di chiusura delle correlate raccomandazioni e in occasione delle successive missioni in argomento. Tra i compiti attribuiti, rientra anche la verifica, ex art. 34 del decreto antiriciclaggio, dell'allineamento tra i sistemi contabili gestionali/settoriali (i.e. i sistemi della Compagnia ove le informazioni vengono registrate per poi essere trasferite in AUI) e quanto deve confluire e materialmente viene trasferito per l'alimentazione dell'AUI o dei sistemi di conservazione dei dati antiriciclaggio.

La Funzione è tenuta a relazionare l'Organo Amministrativo, e l'organo di controllo, dando evidenza delle risultanze dell'attività di controllo svolta. Tale reportistica viene predisposta tenuto conto dell'aspetto di riservatezza connesso alla segnalazione di operazioni sospette e, quando necessario, con un "piano di attività" e un "piano di intervento" dettagliato che possa essere esaminato per la deliberazione e il, conseguente, affidamento all'Organo con funzione di gestione per il monitoraggio e l'assegnazione di delega ai dirigenti preposti alle aree impattate dagli interventi.

4. Analisi e valutazione del rischio di riciclaggio e finanziamento del terrorismo

4.1 Autovalutazione del rischio di riciclaggio e finanziamento del terrorismo

La Funzione antiriciclaggio, secondo quanto disposto dall'art. 14 del Regolamento IVASS n. 44 (come modificato dal Provvedimento IVASS n. 111/2021), coordina ed effettua ogni attività di valutazione, ponderazione del rischio e di analisi inerente all'**esercizio annuale di autovalutazione del rischio di riciclaggio e finanziamento del terrorismo** ("autovalutazione") cui l'impresa è esposta. I risultati di tale esercizio ed il piano delle azioni correttive da intraprendere (ivi inclusa la verifica dello stato di attuazione delle iniziative assunte in precedenza) sono approvati dal Consiglio di Amministrazione

La natura, la portata e la complessità del rischio di riciclaggio, individuato tramite l'autovalutazione, sono esaminati, approfonditi e posti alla base delle determinazioni della Funzione AML a supporto del Consiglio di Amministrazione nell'ambito della definizione di un adeguato sistema di governo societario della Compagnia.

L'autovalutazione viene condotta secondo un **approccio cd. "bottom-up" e mediante una cartografia integrale dei rischi** che renda possibile avere una visione dell'esposizione al rischio della Compagnia suddivisa **per ramo di attività** (i.e. portafoglio di polizze individuali e collettive e di ramo assicurativo) e **per famiglie di prodotto**.

L'esercizio è articolato in tre principali **fasi**:

- determinazione del rischio intrinseco;
- valutazione dei controlli;
- determinazione del rischio residuo.

Determinazione del rischio intrinseco

Il rischio intrinseco viene determinato sulla base del valore assunto da una serie di **fattori di rischio rilevanti** per le imprese (cui è associato un peso diverso in relazione al grado di rilevanza attribuito) individuati sulla base di quanto richiesto da IVASS nonché rilevati da fonti esterne (e.g. pubblicazioni FATF). Tali fattori di rischio, sono riconducibili a tre **principali driver di analisi**:

- Clienti
- Transazioni
- Canali distributivi

A ciascun fattore di rischio viene attribuito un **rating**, attraverso la combinazione di:

- Frequenza, calcolata come incidenza media ponderata della numerosità associata a ciascun fattore di rischio considerato rispetto al numero totale dell'impresa;
- Impatto, determinato come incidenza media ponderata degli importi associati a ciascun fattore di rischio considerato, rispetto al totale dell'impresa;

La combinazione delle suddette variabili consente di determinare il **rating da attribuire ai fattori di rischio individuati** e, conseguentemente, il **rischio intrinseco associato**, che deve essere ricondotto ad una delle **quattro categorie di rischio** di seguito indicate:

- Basso
- Medio-basso

- Medio-alto
- Alto

Valutazione dei controlli

La valutazione del grado di vulnerabilità dei controlli è volta a misurare l'**idoneità dei presidi aziendali** (assetto organizzativo e sistema dei controlli interni) a **ridurre il grado di esposizione al rischio**. Tali presidi sono riconducibili alle seguenti **aree tematiche**:

- Governo societario (*governance*)
- Presidi organizzativi antiriciclaggio (AML Unit)
- Identificazione e verifica della clientela (KYC & Due Diligence)
- Segnalazione delle operazioni sospette (SAR findings)
- Conservazione dei dati e delle informazioni (Record Keeping)
- Monitoraggio costante e controlli (Monitoring)
- Formazione (Training)
- Flussi informativi (Reporting)
- Disponibilità dati (Data enrichment)

L'analisi deve tener conto dell'esistenza o meno del presidio, nonché della sua corretta formalizzazione, implementazione e funzionamento e di ogni eventuale indicazione, suggerimento e/o evidenza di criticità delle altre Funzioni di Controllo e/o che risulti contestata e/o concordata a seguito di verifiche ispettive da parte dell'Autorità di Vigilanza.

In tale fase è, pertanto, necessario assegnare un giudizio motivato ad ogni singolo controllo previsto, nonché descrivere e documentare (a beneficio della sostenibilità della valutazione svolta e per ogni Autorità richiedente) i gap identificati e le eventuali azioni di miglioramento.

La **vulnerabilità così misurata** deve essere ricondotta ad una delle seguenti **categorie**:

- Non significativa;
- Poco significativa;
- Abbastanza significativa;
- Molto significativa.

Determinazione del rischio residuo

Per la determinazione del rischio residuo si applica la matrice indicata da IVASS e di seguito riportata, costruita sulla base della combinazione dei giudizi sul rischio intrinseco e sulla vulnerabilità dei controlli.

Rischio intrinseco	alto				rischio residuo elevato
	medio – alto			Rischio residuo medio	
	medio – basso		Rischio residuo basso		
	basso	Rischio residuo non significativo			
		non significativa	Poco significativa	Abbastanza significativa	Molto significativa
		Vulnerabilità insite nel sistema organizzativo e dei controlli			

Applicando la matrice proposta da IVASS, la determinazione del rischio residuo, sia per le tipologie di prodotto assicurativo considerate sia per la Compagnia nella sua interezza, può assumere i seguenti **valori**:

- Non significativo
- Basso
- Medio
- Elevato

comportando l'adozione di conseguenti misure di adeguamento.

4.2 Risk Assessment

La Funzione Antiriciclaggio, oltre a provvedere ad effettuare l'esercizio di Autovalutazione del grado di esposizione ai rischi di riciclaggio e di finanziamento del terrorismo, nel corso dell'anno, svolge ulteriori esercizi di *assessment* del *framework* in materia di antiriciclaggio/antiterrorismo, nonché di conformità alle sanzioni finanziarie internazionali, eseguiti secondo metodologie sviluppate dal Gruppo BNP Paribas.

Nello specifico sono previsti i seguenti esercizi:

- *Risk & Control Self Assessment* (RCSA): per la valutazione dei rischi di conformità, coordinato dalla Funzione OPC nell'ambito del quale la Funzione Antiriciclaggio, per le parti di competenza, esegue un'attività di Check & Challenge rispetto ai rischi emersi dalle analisi delle funzioni di *business* in tema antiriciclaggio. Gli esiti di tale esercizio sono sottoposti alla validazione dell'Amministratore Delegato della Compagnia.
- *ML/TF Risk classification*: con l'obiettivo di identificare il rischio inerente valutato sulla base di un questionario di autovalutazione che prende in considerazione i seguenti principali *driver*: (i) la tipologia dei prodotti e servizi offerti; (ii) i canali di intermediazione attivi; (iii) le tipologie delle transazioni; (iv) la tipologia della clientela in portafoglio.
- *Annual Global OFAC Sanctions Risk Assessment* (AGORA): con l'obiettivo di identificare e valutare il *framework* da un punto di vista dell'esposizione ai rischi connessi alle Sanzioni Finanziarie ed Embarghi.
- *Cartography, Repository & Reporting Questionnaire* (c.d. CARE2), consistente in una mappatura dei *tool* adottati e dei processi operativi implementati in ambito financial security, le cui evidenze non danno origine ad una valutazione separata, ma vengono parzialmente tenute in considerazione nella definizione dei risultati dell'esercizio AGORA e RCSA.

5. adeguata verifica e valutazione del rischio

5.1. Adeguata verifica e valutazione del rischio di terze parti

L'analisi del rischio di "terze parti", intese come gli intermediari dei quali la Compagnia si avvale nella commercializzazione di prodotti assicurativi tramite un modello di distribuzione definito B to B to C, che entrano in relazione ovvero svolgono compiti e/o effettuano attività per conto della Compagnia è considerato fattore rilevante per una efficace pre-determinazione del rischio e monitoraggio dello stesso.

Al riguardo, il processo aziendale "Know Your Intermediary" definisce i principi, le responsabilità e i processi interni da applicarsi per l'accettazione di un intermediario prima di avviare una nuova relazione di business con quest'ultimo e/o in occasione del monitoraggio attivo della relazione definendo così i requisiti che devono essere rispettati al fine della prevenzione dei rischi di riciclaggio e di contrasto al finanziamento del terrorismo.

Tale processo si compone delle seguenti principali fasi:

1) **Processo di Accettazione Intermediari: avvio del processo**

1.1. Definizione della tipologia di intermediario. È effettuata una preliminare verifica atta ad accertare sia la tipologia e natura dell'Intermediario (e l'assoggettamento a requisiti di Vigilanza di settore) sia anche l'eventuale appartenenza al Gruppo BNP Paribas dell'intermediario al fine di considerare l'uniformità agli stessi principi, regole e/o disposizioni aziendali, oltre che di sottoposizione a verifiche periodiche finalizzate ad accertare il mantenimento della conformità;

1.2. Raccolta di tutta la documentazione necessaria all'avvio della *due diligence* del nuovo Intermediario:

- In caso di accettazione di un intermediario Entità del Gruppo BNP Paribas, si applica la "due diligence" semplificata che prevede un set di controlli di sicurezza finanziaria[17], senza la necessità di formalizzare i dati nell'ambito del "KYI Form"(cfr. punto 1.3. del presente paragrafo).
- In caso di accettazione di un intermediario non appartenente al Gruppo BNP Paribas, le attività da porre in essere consistono nella raccolta di una serie di documentazione richiesta dal KYI Tool alla tabella "Mandatory Documentation" e nella compilazione del KYI Form (al fine di generare la griglia automatica di punteggio, come di seguito indicato), nonché nella raccolta di tutte le informazioni aggiuntive che possono ritenersi importanti per la decisione di avvio della relazione.

1.3. Determinazione del "*risk scoring*" per gli Intermediari non appartenenti al Gruppo BNP Paribas, è richiesta la corretta compilazione del KYI Form affinché lo "scoring" di rischio venga calcolato correttamente e generi in automatico un punteggio complessivo di rischio generato sulla base di una ponderazione degli ambiti di rischio valorizzati nell'algoritmo di calcolo. In casi particolari (i.e. presenza di PEP, rischio reputazionale dell'intermediario, Paese a rischio dove ha sede l'intermediario, ecc.), potrebbe essere richiesto di avviare un Processo Decisionale di livello superiore necessario per l'approvazione dell'Intermediario.

1.4. Esecuzione della "*due diligence*":

1.4.1. Nel caso in cui l'Intermediario sia parte del Gruppo BNP Paribas, risultando quale entità già tenuta all'osservanza delle medesime regole, principi e controlli, il processo prevede, come sopra specificato, l'applicazione della "Due Diligence Semplificata" quale misura richiesta a verificare l'effettiva sussistenza delle condizioni dei requisiti di Legge e/o regolamentari a conferma (o rettifica) del livello di sensibilità attribuito in automatico come "LOW/BASSO";

1.4.2. Per gli Intermediari Esterni ovverosia non appartenenti al Gruppo:

[17] I controlli consistono nella verifica circa la presenza della (i) clausola di sicurezza finanziaria all'interno dell'accordo distributivo sottoscritto, di (ii) eventuali PEPs tra i soggetti correlati all'intermediario, della (iii) eventuale corrispondenza degli stessi soggetti all'interno delle liste sanzioni nonché della (iv) eventuale esistenza di notizie pregiudizievoli.

- In caso di esito di sensibilità LOW o MEDIUM, viene effettuata una due diligence standard;
- In caso di esito di sensibilità HIGH, viene effettuata una due diligence rafforzata.

1.4.3. Esecuzione delle verifiche sui titolari effettivi, in conformità alla classificazione di rischio, tempo per tempo attribuita, mediante accesso e consultazione del registro dei titolari effettivi.

2) Ri-certificazione periodica degli Intermediari:

Gli intermediari sono sottoposti ad un processo di revisione periodica (cd. "on-going due diligence") con cadenza regolare, la cui periodicità viene definita sulla base del livello di sensibilità attribuito all'intermediario stesso al momento dell'accettazione o dell'ultima revisione.

Al momento della ri-certificazione, le misure di Due Diligence, in aggiunta a quelle richieste in fase di accettazione, prevedono un confronto tra:

- l'andamento della relazione di business al momento della ri-certificazione ed il risultato previsto al momento dell'instaurazione della relazione con l'intermediario;
- laddove applicabile, l'andamento totale dell'Asset under Management ("AuM") dei clienti al momento della ri-certificazione e quello previsto al momento dell'instaurazione del rapporto di intermediazione;
- la valutazione sui clienti in portafoglio al momento della ri-certificazione.

5.2. Adeguata verifica e valutazione del rischio della clientela

L'esecuzione delle attività di adeguata verifica è disposta sia per le **polizze individuali** sia per quelle **collettive** e si applica a tutti coloro che (siano essi persone fisiche o soggetti differenti da persone fisiche/entità) rientrano nella definizione di Cliente, risultando a disporsi:

- quale condizione essenziale per poter **instaurare un rapporto continuativo,** ovvero **in caso di modifica di elementi afferenti alla titolarità del rapporto (ad es. cambio contraenza) o inerenti alla prestazione**, quindi, allorquando viene **designato un beneficiario** o viene **liquidata la prestazione assicurativa**;
- al **compimento di specifiche operazioni**, qualora vi sia un soggetto terzo pagatore, un terzo percipiente (nei casi previsti dalla normativa aziendale – in caso di sinistro) o vi siano variazioni/ introduzioni di soggetti collegati al rapporto (i.e. nuovo titolare effettivo);
- se vi è **sospetto di riciclaggio**, indipendentemente da qualsiasi deroga, esenzione o soglia applicabile;
- nei confronti dei nuovi clienti, nonché dei clienti già acquisiti, quando accade un evento suscettibile di influenzare il livello di rischio (c.d. "ri-certificazione ad evento") e, in ogni caso, secondo una frequenza predeterminata in ragione della classe di rischio assegnata (c.d. "ri-certificazione periodica"), salvo eccezioni.
- nei confronti dei clienti già acquisiti, alla prima occasione utile e/o in ragione del profilo temporale attribuito in considerazione del livello di rischio o qualora sia individuata una non conformità o un *alert*.

L'**adeguata verifica** della clientela consiste nelle seguenti **attività**:

- **identificazione** del **cliente e dei soggetti ad esso connessi**, del **beneficiario** (incluso il percipiente), dell'eventuale terzo pagatore e dell'eventuale **esecutore**, nonché dell'eventuale **titolare effettivo** del cliente e del **beneficiario**;
- **verifica dell'identità** dei soggetti di cui al punto precedente sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile ed indipendente ed anche mediante accesso al "registro di titolarità effettiva" per il riscontro della veridicità dei dati e delle informazioni dichiarate sui "titolari effettivi";
- acquisizione e valutazione di **informazioni su scopo e natura del rapporto continuativo**;

- esercizio di un **controllo costante nel corso del rapporto continuativo (anche sulle modifiche di titolarità effettiva)**.

La modulazione dell'**intensità** e dell'**estensione degli obblighi di adeguata verifica avviene in base al grado di rischio** di riciclaggio e di finanziamento del terrorismo del cliente o dell'operazione (**approccio basato sul rischio**).

In ragione degli "eventi di rischio" individuati, l'esecuzione del processo di Adeguata Verifica potrà avvenire in modalità ordinaria, semplificata o rafforzata. Per la **valutazione del rischio** si terrà conto dei **fattori** e degli **elementi di rischio** associati al **cliente**, al **rapporto continuativo** all'**operazione e al tipo di prodotto** indicati nella normativa nazionale ed internazionale applicabile, nonché di quelli individuati a livello di Gruppo.

Fatti salvi i casi per i quali è richiesta e/o sussistono le condizioni per l'applicazione dell'adeguata verifica rafforzata, il modello di rischio prevede:

- **Prodotti Saving**: applicazione di misure di adeguata verifica ordinaria
- **Forme pensionistiche**: applicazione di misure di adeguata verifica semplificata
- **Prodotti Protection**: applicazione di misure di adeguata verifica semplificata

sia nel caso di delega allo svolgimento di parte delle attività di adeguata verifica agli intermediari costituenti la propria rete distributiva (tenuti a sottoporre i casi di "adeguata verifica rafforzata" alla Compagnia) sia per i cosiddetti "clienti diretti"[18] per i quali il processo di adeguata verifica è gestito direttamente dall'impresa.

I sistemi valutativi ed i processi decisionali adottati devono assicurare **coerenza di comportamento** all'interno della struttura aziendale e la **piena tracciabilità delle verifiche svolte** e **delle valutazioni effettuate**, anche al fine di dimostrare alle Autorità competenti che le specifiche misure assunte sono adeguate rispetto ai rischi rilevati nel concreto.

3.2.9 Acquisizione di dati e informazioni

Gli intermediari sono responsabili in proprio della raccolta delle informazioni e della documentazione ai fini dell'adeguata verifica sulla base delle istruzioni, tempo per tempo, fornite dalla Compagnia tenendo conto del livello di rischio del prodotto, ad eccezione per i "clienti diretti" per i quali la Compagnia svolge direttamente tali attività.

Prodotti Saving

Devono essere acquisiti **dati ed informazioni** anche ai fini della determinazione del grado di rischio, mediante **procedure logiche e valutazioni strutturate** (i.e. su valutazione dei principali eventi di rischio) attraverso l'acquisizione dei dati e delle informazioni tramite l'utilizzo di **questionari/modulistica** differenziata in base al tipo di cliente e/o operazione e alla loro rischiosità.

L'acquisizione dei dati e delle informazioni mediante dichiarazioni del Cliente costituisce condizione **obbligatoria** per poter proseguire con l'**apertura del rapporto continuativo**, con la **liquidazione della prestazione assicurativa** o il **compimento di specifiche operazioni** (i.e. cambio di contraenza, cambio di beneficiari, versamenti aggiuntivi, riscatti totali/ parziali, recesso, revoca)[19].

[18] La Compagnia opera principalmente nella modalità di distribuzione B to B to C, raramente la Compagnia entra in relazione diretta con i propri clienti finali (c.d. clientela diretta), ad eccezione dei clienti interni (dipendenti della Compagnia a cui è riservata una specifica polizza, normata da una procedura dedicata).
Un'ulteriore casistica riguarda la gestione post vendita dei cd "clienti diretti esterni", ovverossia clienti entrati inizialmente in relazione per il tramite di Terzi Intermediari poi passati in una fase successiva alla gestione operativa diretta della Compagnia.

[19] La modulistica utilizzata, differenziata per persona giuridica o persona fisica, consiste in specifici questionari di adeguata verifica per i casi di i) nuova emissione ii) riscatto totale e parziale, iii) liquidazione. Per ciascuna fase del rapporto continuativo è prevista esclusivamente la raccolta dei dati dei soggetti nella stessa coinvolti. I moduli di riscatto e liquidazione sono integrati con l'attestazione status ai fini FATCA e AEOI.

Nell'ambito dello svolgimento della "adeguata verifica" viene dato risalto all'attività di identificazione e verifica ed all'acquisizione dei dati e delle informazioni su scopo e natura del rapporto con la finalità di pervenire alla **determinazione del profilo di rischio** della clientela che sia rivolta:

(→) al **cliente e includa tutte le persone associate direttamente al cliente e/ o indirettamente al rapporto**, la cui natura può variare in relazione al segmento di appartenenza.

In particolare, costituiscono elemento idoneo alla corretta effettuazione dell'adeguata verifica l'analisi circa i titolari effettivi ("*beneficial owners*") ed i criteri utilizzati per la loro individuazione, i firmatari autorizzati/ delegati ad operare (esecutori) e i beneficiari di contratti di assicurazione sulla vita. La necessità di identificare ulteriori persone associate è definita nell'ambito delle policies per segmento di clientela.

Le **macro-categorie di informazioni raccolte** fanno principalmente riferimento a[20]:

- **dati identificativi** ed **altri dati anagrafici** completi (inclusi i dati fiscali e di residenza e domicilio);
- **prevalente attività economica svolta** e **localizzazione della stessa**, nonché **relazioni economiche e commerciali con l'estero**;
- carica di **Persona Politicamente Esposta e/o qualifica di Politico Italiano Locale (PIL), anche a seguito e in dipendenza dell'esercizio di funzioni direttive e/o svolgimento di attività con la Pubblica Amministrazione e/o entità qualificabili come "pubbliche"**;
- **assetto societario di gruppo** e approfondimenti necessari in caso di entità con caratteristiche di cd. "maggior rischio" (i.e. presenza nella catena partecipativa di trust, fiduciarie o società anonime e nazionalità delle stesse, fondazioni o ONLUS);
- **legami** tra i principali soggetti coinvolti (i.e. tra cliente ed esecutore; tra cliente e beneficiario designato; tra cliente ed assicurato; tra assicurato e beneficiario designato; tra cliente e titolare effettivo sub 2); tra cedente del rapporto e nuovo cliente);
- **scopo** e **natura del rapporto** continuativo;
- **tipologia** e **Paese di provenienza dei fondi** utilizzati per l'apertura del rapporto continuativo o nell'operazione;
- **Paese di destinazione dei fondi** in occasione della liquidazione della prestazione assicurativa;
- **situazione lavorativa**, **economica** e **reddituale** e **patrimoniale**;
- **importo** e **mezzo di pagamento** delle operazioni.

Con riferimento ai dati identificativi di cui sopra, rispettivamente, le verifiche avvengono (per il tramite dell'Intermediario Assicurativo, ovvero, nei casi previsti, direttamente dalla Compagnia):

- **per i soggetti persone fisiche**, mediante riscontro con le informazioni contenute nel documento di identità o in documenti di riconoscimento equipollenti ai sensi della normativa vigente;
- **per i soggetti persone non fisiche/entità**, effettuando il riscontro dei dati identificativi con le informazioni desumibili da fonti affidabili ed indipendenti, acquisite in via autonoma o dal cliente o dal beneficiario, conservandone copia in formato cartaceo o elettronico. Con riferimento alla titolarità effettiva, si adottano misure proporzionate al rischio per ricostruire l'assetto proprietario e di controllo del cliente/ beneficiario, consultando ogni fonte informativa per individuare il titolare effettivo;
- **per l'esecutore**, acquisendo documenti volti ad appurare la sussistenza del potere di rappresentanza in forza del quale egli opera in nome e per conto del cliente o del beneficiario.

Qualora in ambito dell'attività di verifica dovessero emergere dei dubbi sono effettuati ulteriori **approfondimenti** e la valutazione di eventuale segnalazione di operazione sospetta.

[20] Le informazioni riportate non sono raccolte indistintamente per tutti i soggetti coinvolti nel rapporto continuativo/ operazione, bensì variano a seconda della tipologia di controparte ed operazione (e.g. cliente persona fisica o cliente persona giuridica, beneficiario diverso dal contraente, esecutore, pagamento di premi da parte di un terzo soggetto diverso dal contraente, liquidazione della polizza a favore di un percipiente, ecc.).

In aggiunta a quanto sopra, agli operatori degli intermediari che entrano in contatto con la clientela e a Cardif Vita è richiesto di **esprimere una valutazione qualitativa** tramite la **raccolta di ulteriori informazioni** quali a titolo esemplificativo: il comportamento tenuto dal cliente/ esecutore, informazioni sfavorevoli/pregiudizievoli, etc.

Forme pensionistiche e Prodotti Protection

Ai fini dell'attività di acquisizione di dati e informazioni valgono le medesime considerazioni sopra descritte per i Prodotti Saving, tenuto in considerazione che in applicazione di misure di adeguata verifica semplificata, i questionari antiriciclaggio sono coerenti con il livello informativo richiesto.

3.2.10 Determinazione del profilo di rischio della clientela

Il rischio connesso a un rapporto d'affari si compone del **rischio intrinseco** relativo al **cliente**, del rischio relativo ai **prodotti**, alle **operazioni** e al **canale di distribuzione**, e del rischio relativo ai **fattori geografici**.

Il **profilo di rischio della clientela** è **determinato conformemente alla metodologia di rischio stabilita dalla Compagnia, sulla base dei dati e delle informazioni acquisiti** tramite il Questionario antiriciclaggio per l'adeguata verifica del cliente e del beneficiario e/o la modulistica richiesta in fase di compimento di specifiche operazioni, **nonché degli esiti della consultazione delle liste antiriciclaggio e antiterrorismo**.

La Compagnia si è dotata di un **apposito modulo informatico (cfr. "Classifier"**) per assolvere agli adempimenti di adeguata verifica previsti dal D.lgs 231/07 e ss. m e i. al fine di pervenire alla puntuale valutazione di ogni dato, informazione e/o elemento e così provvedere ad assegnare i pertinenti profili di rischio di riciclaggio.

Tale strumento, declinato in conformità all'approccio basato sul rischio quindi alle regole[21] adottate dalla Compagnia, attualmente, tiene in considerazione gli "eventi di rischio iniziali", tempo per tempo previsti dalla normativa.

In particolare, anche in recepimento delle *best practices* indicate da EBA-ESMA ed EIOPA, ha quale presupposto i rischi associati:

i- al "*cliente*" (ad es. attività svolta, reddito, qualifica - PePs. e/ o condotta),

ii- al "*prodotto*" (risparmio, protezione e forme pensionistiche),

iii- alle "*operazioni*" (ad es. importi dei pagamenti premi e area/regione di operatività e congruità/ ragionevolezza dell'operazione rispetto al profilo economico del cliente - i.e asset investiti/ patrimonio), così come acquisite attraverso i questionari di "adeguata verifica", anche avendo in considerazione i cd. "*canali distributivi*" (i.e. in prevalenza mediante bancassurance) - che hanno propri criteri di valutazione e determinazione del rischio e dei controlli,

iv- ai "*Paesi controparte*" per ogni operazione di liquidazione e/ o incasso che sia destinata/ proveniente verso/ da Paesi "non cooperativi" ovvero assoggettati a sanzioni finanziarie e/ o soggetti con conti e/ o domicilio e/ o residenza in detti Paesi.

Il **modello di profilatura assegna a ciascun cliente una specifica classe di rischio a cui sono associati i relativi livelli di vigilanza,** previo controllo e/o verifica della Funzione Antiriciclaggio sugli eventi sottoposti ad "adeguata verifica rafforzata", come di seguito indicato:

Livello di rischio		Livello di Vigilanza
0	Irrilevante	Adeguata verifica semplificata

[21] Artt. 15 e 17 D. Lgs. N. 231/07.

Livello di rischio		Livello di Vigilanza
1	Basso	Ordinario
2	Medio	Ordinario
3	Alto	Rafforzato

La natura e la portata delle misure di cd. "validazione e/o modifica della classe di rischio" sono adeguate al livello di rischio.

In particolare:

- un "livello di rischio alto" richiede un'intensificazione delle misure di verifica e un processo decisionale con l'intervento del Comitato Accettazione Clienti/KYC Review o del Comitato Antiriciclaggio.

  Il rafforzamento delle misure può anche verificarsi, conformemente ad un approccio "*case by case*" in caso di (ad esempio):

  - evento di rischio intervenuto;
  - di attribuzione di un profilo di rischio "alto" in dipendenza di, eventuali circostanze di rischio che il Responsabile della Funzione AML decida di sottoporre ad approfondimenti;

- un "livello di rischio irrilevante" consente una semplificazione delle misure di verifica e del processo decisionale, conformemente alla normativa applicabile.

Il modello di profilatura è strutturato in ragione dell'**attribuzione di un punteggio che è oggetto di integrazione laddove si presenti un elemento di rischio che comporti una variazione a rialzo dello stesso**. Il livello finale comporta l'esecuzione di eventuali approfondimenti laddove detto livello risulti essere "alto".

L'algoritmo con i criteri di rischio e le logiche di assegnazione di rilevanza ai "fattori/eventi/di rischio" viene sottoposto a una periodica revisione da parte della Funzione Antiriciclaggio sulla base dell'operatività e della tipologia di prodotti con un'ottica di mantenimento del più corretto e congruo approccio al rischio.

In tale contesto, è compito della Funzione Antiriciclaggio valutare l'adeguatezza dei sistemi informativi e delle procedure interne volti:

i. all'adempimento degli obblighi di adeguata verifica della clientela ed
ii. alla rilevazione, valutazione e segnalazione delle operazioni sospette,

riportando all'attenzione e determinazione del Comitato di Sicurezza Finanziaria ogni modifica e/o criticità e/o miglioria che si ritenga opportuno adottare.

Il livello e l'intensità delle verifiche può essere modificato in conseguenza della rilevazione di un fattore di rischio che risulti più elevato nel corso del processo di raccolta di informazioni e di adeguata verifica. (Per maggiori dettagli sull'attuazione delle misure di verifica, è bene fare riferimento alle Policy KYC in vigore).

La Funzione Antiriciclaggio, fermi i casi di "adeguata verifica rafforzata" e/o "eventi di rischio specifici" che richiedono un approfondimento, mantiene sempre la **possibilità di determinare l'applicazione di un regime di adeguata verifica differente da quello automaticamente stabilito dal sistema informativo**, sulla base di attività di controllo svolte sulla clientela, accertamenti, notizie pregiudizievoli, nonché di esprimere valutazioni in merito alla coerenza del rapporto/ operazione rispetto al profilo socio-economico del cliente, alla documentazione fornita ed al comportamento tenuto dal cliente/ esecutore/ beneficiario.

Il **livello di rischio** è, pertanto, determinato in **due fasi**:

- **una valutazione o "*scoring*" basata su criteri obiettivi o quantificabili** – il che consente di automatizzare il processo o di farlo eseguire da un Team operativo KYC;
- **la presa in considerazione di elementi qualitativi** che richiedono un'analisi o un giudizio.

3.2.11 Misure semplificate di adeguata verifica

Possono essere adottate delle misure di verifica semplificata (che non sono misure di esenzione, bensì di una acquisizione di dati e informazioni meno estesa rispetto alla adeguata verifica ordinaria) al momento dell'apertura del rapporto d'affari per determinate categorie di clienti, rapporti, prodotti o servizi purché sussistano e siano documentabili le condizioni e caratteristiche specificamente definite dalla normativa e dalla regolamentazione attuativa.

Coerentemente con i principi disciplinati dall'articolo 23 del Decreto antiriciclaggio, la Funzione Antiriciclaggio potrà applicare **misure semplificate** di adeguata verifica ai clienti, alle controparti e per l'instaurazione dei rapporti, intendendo le stesse sotto il profilo dell'estensione (in termini di acquisizione di dati, informazioni, approfondimenti e riscontri) e della frequenza degli adempimenti prescritti dall'articolo 18 del medesimo Decreto.

Le condizioni necessarie per l'applicazione sono:

- (di cd. "natura soggettiva") Quando **il cliente** rientra nelle seguenti categorie:
  - Banche e istituti finanziari con sede in uno Stato noto a livello internazionale e, conseguentemente, a BNP Paribas, per l'imposizione di obblighi equivalenti a quelli imposti dalla regolamentazione europea e francese.
  - Società e loro succursali e controllate al 100%, quotate su mercati azionari noti a BNP Paribas per imporre (tramite regolamenti di mercato o regolamentazione) obblighi appropriati in materia di trasparenza sul titolare effettivo.

- (di cd. "natura oggettiva") Qualora il cliente utilizzi esclusivamente i **prodotti di** seguito elencati:
  - Prodotti di protezione.
  - Contratti di assicurazione pensionistica che non prevedono la clausola di riscatto, non possono essere utilizzati come garanzia e quindi vengono ritirati come rendita al momento del pensionamento, come alcune assicurazioni temporanee in caso di decesso, rendite vitalizie, contratti di previdenza, salute e pensione integrativa.

In tali casi, salvo che non vi sia altro e/o differente motivo per sottoporre il cliente ad "adeguata verifica rafforzata", ovvero non vi sia alcun e/o ulteriore o sopraggiunto sospetto di riciclaggio di denaro, la procedura di adeguata verifica sarà semplificata e, in senso coerente, potrà procedersi alla valutazione del rischio come "IRRILEVANTE/BASSO".

Le misura di adeguata verifica semplificata consistono in:

- **una riduzione della quantità/estensione delle informazioni documentate da raccogliere**, incluse la verifica dell'identità del titolare effettivo sub 2) attraverso una dichiarazione sottoscritta dal cliente oppure l'individuazione tramite presunzioni dello scopo e della natura del rapporto continuativo, laddove il contratto di assicurazione sia univocamente destinato alla copertura di uno specifico rischio;

- **una riduzione della frequenza dell'aggiornamento dei dati raccolti ai fini dell'adeguata verifica**, prevedendo che venga effettuato solo al ricorrere di eventi che possano modificare l'attribuzione del profilo di rischio, quali l'apertura di un nuovo rapporto continuativo;

- **una riduzione della frequenza e della profondità di analisi funzionali al monitoraggio del rapporto**.

Costituiscono condizioni ostative per cui, ove individuate, **non si provvede all'applicazione di misure semplificate, ovvero (in caso di condizioni sopraggiunte) il cliente debba essere ri-sottoposto ad adeguata verifica "ordinaria" o "rafforzata"** qualora:

- siano **emersi riscontri positivi e/o eventi di rischio** a seguito delle attività di ***customer screening o customer/transaction monitoring***;

- l'operatore **ritenga** che allo stesso **debba essere applicata l'adeguata verifica ordinaria o rafforzata** e, in tal senso, proponga la posizione al Responsabile della Funzione Antiriciclaggio.

Ci si dovrà astenere **dall'applicare misure semplificate** di adeguata verifica laddove:

- sussistano dubbi, incertezze o incongruenze in relazione ai dati identificativi e alle informazioni acquisite in sede di identificazione del cliente, del beneficiario nonché dei rispettivi esecutori o titolari effettivi, ovvero
- **vengano meno le condizioni** per l'applicazione delle misure semplificate (e.g. incremento del profilo di rischio del cliente a causa di variazione delle informazioni acquisite per clienti e soggetti collegati; match accertati a seguito delle attività di customer screening; operazioni di versamento aggiuntivo il cui importo comporta il superamento di determinate soglie);
- il controllo costante sulla complessiva operatività del cliente e le informazioni acquisite nel corso del rapporto inducano a **escludere la presenza di una fattispecie a rischio irrilevante**;
- vi sia comunque il **sospetto di riciclaggio o di finanziamento del terrorismo**.

3.2.12 Misure rafforzate di adeguata verifica

In presenza di un **alto rischio di riciclaggio**, risultante da specifiche previsioni normative (cfr. articolo 46 Regolamento IVASS n. 44), ovvero dall'autonoma valutazione condotta sulla base dell'approccio basato sul rischio, nonché a seguito di allineamento con il livello di rischio più elevato definito su un comune cliente da un'altra entità del Gruppo, si dovrà procedere ad **applicare misure rafforzate di adeguata verifica della clientela**, caratterizzate dall'adozione di presidi aventi **maggiore profondità, estensione e/o frequenza**.

La presenza di un alto rischio di riciclaggio può essere dipendente sia da fattori connessi ad "eventi pregiudizievoli" sia da "elementi di rischio" indicati dalle "Linee Guida EBA-ESMA ed EIOPA" sia anche individuati dalla normativa di Gruppo e/o locale.

Nello specifico gli elementi legati al cliente e considerati **scatenanti** (con "eventi bloccanti" che richiedono una specifica e motivata autorizzazione da parte della Funzione Antiriciclaggio) sono, tra gli altri:

- presenza nelle liste terroristi;
- precedenti valutazioni positive di operazioni sospette (in tal caso evento "bloccante" salvo motivate considerazioni da parte del Delegato SOS e del Responsabile della Funzione AML);
- presenza in liste *crime* (notizie pregiudizievoli);
- status di Persona Politicamente Esposta inclusi i rapporti e/o legami dipendenti dallo svolgimento di attività e/o funzioni pubbliche e/o rapporti e/o attività con la Pubblica Amministrazione e/o entità pubbliche che è valutato anche nel caso di "titolarità effettiva";
- presenza di pendenze giudiziarie (soprattutto di natura penale e/o la conoscenza diretta di indagini -ad es. ricezione di notifica di un decreto o atto dell'Autorità);
- presenza di incidenti di sicurezza finanziaria;
- tipologia di entità/*legal arrangements* (ONLUS, enti non profit, società fiduciaria, trust);
- comportamento cliente (reticenza nel fornire informazioni, poca trasparenza nella struttura di controllo, operazione effettuata con modalità non usuali, interposizione di terzi senza motivazione);
- il cliente persona giuridica è costituito in un Paese ad alto rischio (HS/VHS) nel quale BNP Paribas non è presente;
- il cliente risiede in un Paese "Major Sanctioned Countries" - MSC, o almeno il 5% della sua attività interessa un Paese MSC;
- un titolare effettivo risiede in un Paese MSC.

La **presenza di almeno uno degli elementi scatenanti** può determinare l'attribuzione di un profilo al cliente pari ad Alto che richiede l'intervento consultivo ed anche autorizzativo della Funzione AML.

È, comunque, disposto che la Funzione Antiriciclaggio **possa decidere mediante apposito provvedimento di applicare** comunque **il regime rafforzato** anche qualora non ricorrano gli elementi scatenanti e per specifiche fattispecie che la stessa Funzione e/o il Responsabile della stessa provvederà a indicare.

L'**adeguata verifica rafforzata** consiste:

- nell'acquisizione **di maggiori informazioni e documentazione** su cliente, beneficiario e soggetti collegati, e sulla **provenienza e destinazione dei fondi**, nonché una più **approfondita valutazione della natura e dello scopo del rapporto**;
- in una **maggiore profondità di analisi** in occasione dell'esecuzione di specifiche operazioni;
- in una **maggiore frequenza degli aggiornamenti** delle informazioni acquisite;
- nel **ritenere sospeso condizionatamente alla qualificazione del rischio** (da valutare come accettabile in aderenza al *risk appetite framework* e all'avvenuta rimozione di indici di rischio significativi per come, originariamente, individuati) **l'apertura del rapporto od il compimento dell'operazione**;
- nell'**intervento della Funzione Antiriciclaggio e/o la richiesta di indire un Comitato Accettazione Clienti ("CAC") o di un "KYC Review".**

Particolare attenzione va riservata alle **Persone Politicamente Esposte (PEPs)** considerate a più alto rischio di riciclaggio in quanto maggiormente esposte a potenziali fenomeni di corruzione, unitamente ai relativi familiari, come definiti dalla norma, e alle persone che notoriamente sono loro strettamente legate. Nello specifico, il processo per verificare se il cliente, il beneficiario ed i relativi titolari effettivi siano qualificabili come PEPs adottato dal gruppo BNPP si basa essenzialmente sui seguenti elementi:

- informazioni raccolte in sede di adeguata verifica, nonché sulla base della relazione d'affari intrattenuta con il soggetto;
- la piattaforma di Gruppo "Vigilance", utilizzata quando si intraprende una nuova relazione o in sede di ri-certificazione, allo scopo di consultare l'elenco dei PEP ivi presenti, i familiari o i soggetti che con essi risultano avere legami. Questo elenco proviene dalle "liste Factiva" di proprietà della Società del Gruppo Dow Jones Reuters;
- il regolare screening automatico dei database clienti/ relazioni d'affari con l'elenco PEP.

Conformemente alla Policy dedicata[22], il trattamento dei PEP risponde alle seguenti ulteriori regole generali:

- I clienti persone fisiche che sono PEP sono sempre valutati e potenzialmente classificati ad "Alto Rischio".
- I clienti persone giuridiche di cui un titolare effettivo è un PEP sono valutati e potenzialmente classificati ad "Alto Rischio".
- La decisione finale viene sempre assunta a fronte dell'intervento della Funzione Antiriciclaggio o dei Comitati CAC/KYC Review.

  Nello specifico, nell'ambito del processo decisionale della Compagnia, per l'instaurazione del rapporto è previsto che qualora il cliente, il beneficiario o il titolare effettivo risulti essere un PEP, vi debba essere l'approvazione da parte del Comitato Accettazione Clienti, così come nel caso di ricertificazione da parte del Comitato KYC Review.

  Il medesimo iter autorizzativo è previsto anche in merito all'eventuale successiva perdita dello status di PEP o mantenimento del livello di rischio anche per periodi superiori a quanto stabilito dalla Legge applicabile. In caso di movimento post-vendita è invece possibile un'approvazione semplificata da parte della sola Funzione Antiriciclaggio.

- La **prosecuzione** nell'applicazione di **misure di adeguata verifica rafforzata** è, comunque, previsto che avvenga anche successivamente alla perdita di status di PEP in conformità con le procedure interne.

[22] Cfr. Policy CAN 03-03-05 – Relazione con le Persone Esposte Politicamente (PEPs).

- La **verifica**, nell'ambito dell'attività di controllo costante, dell'**eventuale acquisizione** o delle **successive variazioni** dello **status di PEP.**

Conformemente a quanto previsto dalla normativa locale (art. 25 co. 5 del D. Lgs. 231/07 e ss. m. e i.), laddove il beneficiario della prestazione assicurativa o il titolare effettivo del beneficiario siano persone politicamente esposte, la Compagnia applica al momento del pagamento della prestazione ovvero della cessione del contratto, le seguenti ulteriori misure:

- informare l'Amministratore Delegato ovvero i soggetti appositamente delegati e muniti di poteri autorizzativi prima del pagamento dei proventi della polizza;
- eseguire controlli più approfonditi sull'intero rapporto con il contraente.

Assumendo quale criterio interpretativo di legge, scelto dal legislatore UE e richiamato dal legislatore nazionale, il *risk based approach*, quale misura anche per l'assolvimento degli adempimenti antiriciclaggio, viene determinato che la classificazione del rischio abbia un effetto che deve essere applicato in armonia con tutti i fattori di rischio presenti e applicabili (ad es. prodotto e canale distributivo) e ne debba essere fornita una interpretazione sostanziale idonea a migliorare la valutazione preventiva ed anche gli stessi controlli successivi.

Ne consegue come per il cliente PEP che risulti aderente di sole polizze di protezione, tenuto conto del livello di rischio del prodotto e della operatività prevista nell'ambito della vendita dello stesso, la posizione venga esaminata ex post e sottoposta ad adeguata verifica rafforzata solo qualora emergano elementi ulteriori di rischio.

Infine, ai sensi dell'art. 25 co. 4bis del D.lgs. 231/2007 e ss. m. e i., la Compagnia nei casi di rapporti continuativi, prestazioni professionali e operazioni che coinvolgono paesi terzi ad alto rischio, in aggiunta a quanto previsto dal comma 1[23]:

- acquisisce informazioni aggiuntive in merito allo scopo e alla natura del rapporto continuativo o della prestazione professionale;
- acquisisce informazioni sull'origine dei fondi e sulla situazione economico-patrimoniale del cliente e del titolare effettivo;
- acquisisce informazioni sulle motivazioni delle operazioni previste o eseguite;
- acquisisce l'autorizzazione dei soggetti titolari di poteri di amministrazione o direzione o di loro delegati o, comunque, di soggetti che svolgono una funzione equivalente, prima di avviare o proseguire o intrattenere un rapporto continuativo, una prestazione professionale o effettuare un'operazione che coinvolga paesi terzi ad alto rischio;
- assicura un controllo costante e rafforzato del rapporto continuativo o della prestazione professionale, aumentando la frequenza e l'intensità dei controlli effettuati ed individuando schemi operativi da sottoporre ad approfondimento.

3.2.13 Controllo costante nel corso del rapporto continuativo

Nel corso del rapporto continuativo deve essere svolto un controllo costante per **mantenere aggiornato il profilo di rischio** del cliente e per **individuare eventuali elementi di incongruenza** che possano costituire anomalie

[23] Secondo cui "in presenza di un elevato rischio di riciclaggio o di finanziamento del terrorismo, adottano misure rafforzate di adeguata verifica della clientela acquisendo informazioni aggiuntive sul cliente e sul titolare effettivo, approfondendo gli elementi posti a fondamento delle valutazioni sullo scopo e sulla natura del rapporto e intensificando la frequenza dell'applicazione delle procedure finalizzate a garantire il controllo costante nel corso del rapporto continuativo o della prestazione professionale.

rilevanti, al fine di adottare misure rafforzate di adeguata verifica, di astenersi dall'esecuzione dell'operazione o dal consentire modifiche contrattuali oppure di valutare la segnalazione di operazioni sospette.

Il controllo costante è esercitato attraverso l'**esame della complessiva operatività del cliente**, avendo riguardo sia ai rapporti continuativi in essere che alle operazioni specifiche eventualmente disposte, nonché mediante l'**acquisizione di ulteriori informazioni** o l'**aggiornamento delle notizie già possedute.**

In particolare, le **attività di controllo costante** sono riconducibili a:

- individuazione di elementi di incongruenza che possono condurre alla **segnalazione di operazioni sospette**;
- effettuazione di **più ampie e approfondite verifiche** in occasione del compimento da parte del cliente di **operazioni considerate a maggior rischio**;
- esecuzione periodica delle attività di ***customer screening*** su clienti, beneficiari e soggetti collegati;
- aggiornamento di **dati**, **informazioni** e, conseguentemente, del **profilo di rischio** della clientela.

3.2.14 Validità temporale del profilo di rischio

La **frequenza di aggiornamento della profilatura del cliente** (cfr. art. 31 del Regolamento IVASS n. 44) è definita sulla base del relativo livello di rischio, previa valutazione di congruità della classe di rischio assegnata al cliente tenendo conto della eventuale presenza di fattori di rischio (i.e. successiva assunzione della qualifica di persona politicamente esposta, cambiamenti rilevanti dell'operatività del cliente o dell'assetto proprietario o di controllo).

È richiesto e così previsto l'**aggiornamento del profilo di rischio del cliente** (cosiddetta "**ricertificazione dei clienti**"[24]) nei seguenti casi:

- secondo una frequenza determinata dal segmento di clientela e dal livello di rischio del cliente, salvo per i dossier meno rischiosi (c.d. **"ricertificazione periodica"**);
- in caso di eventi suscettibili di influenzare il livello di rischio (c.d. **"ricertificazione ad evento"**).

  La cronologia del rapporto d'affari è documentata e può essere confrontata con le finalità iniziali relative all'accensione del rapporto continuativo e con il profilo transazionale.
- in caso di riscontrate incongruenze informative con il "registro dei titolari effettivi"[25].

3.2.15 Rapporti d'affari vietati e obbligo di astensione

È fatto divieto assoluto di sottoscrivere o proseguire un rapporto d'affari già instaurato che coinvolga tipologie di clienti o situazioni di seguito descritte:

- determinate categorie di "Persone Politicamente Esposte": i capi di Stato o di governo e i membri delle loro famiglie, se sono stati o sono in carica in Paesi a sensibilità elevata ("HS": High Sensitivity) o molto elevata ("VHS": Very High Sensitivity[26]);

[24] Per maggiori dettagli confronta CAN 03.02.01 "KYC General Policy BNP Paribas Cardif versione adattata per Cardif Vita".
[25] Previsione da intendersi effettiva dal momento dell'entrata in vigore del Provvedimento che rende operativo il Registro della Titolarità Effettiva.
[26] I Paesi HS e VHS vengono definiti, tempo per tempo, all'interno delle liste di Gruppo che individuano quali Paesi terzi ad alto rischio quelli individuati come tali dal GAFI e dall'UE, nonché ulteriori giurisdizioni estere valutate sulla base di una metodologia interna che considera diversi fattori di rischio.

- qualsiasi persona fisica o giuridica, in qualità di cliente o soggetto ad esso correlato (beneficiario, esecutore, terzo pagatore, legale rappresentante, etc) oggetto di sanzioni finanziarie internazionali[27];
- Paesi sottoposti a sanzioni: qualsiasi nuovo rapporto con una persona fisica o giuridica residente[28] in un Paese sottoposto a sanzioni (MSC)[29];
- dossier non conformi per assenza o mancata acquisizione (anche in sede di rinnovazione) di dati essenziali ai fini dell'effettuazione/completamento della "adeguata verifica", ovvero esistenza di criticità e/o dubbi;
- CSR: qualsiasi cliente presente nella lista di esclusione CSR e i rapporti d'affari che coinvolgono società che producono, utilizzano e/o commercializzano dei beni, rientranti nella CSR *list*[30] contenente l'elenco dei beni e delle attività escluse.

In dettaglio, in conformità con quanto disposto dall'articolo 42 del D. Lgs. n. 231/2007 e s.m. e i., la Compagnia e gli Intermediari facenti parte della Rete Distributiva diretta della Compagnia stessa applicano, rispettivamente:

(i→) l'astensione dal perfezionamento dal rapporto, ove non siano in grado di espletare le attività di adeguata verifica della clientela, includendo anche la grave incongruenza con i dati di titolarità effettiva dichiarati e quelli presenti nel "registro di titolarità effettiva" (salvo non sussistano adeguate giustificazioni);

(ii→) la risoluzione del rapporto già instaurato, ove non siano in grado di espletare le attività di rinnovazione della adeguata verifica della clientela;

(iii→) la segnalazione da parte del Delegato SOS d'intesa con il responsabile Antiriciclaggio, ovvero l'adozione di altre misure qualora sussistano eventi di rischio e/o pregiudizievoli, in relazione ai quali il Cliente non produca idonea documentazione e/o giustificazioni;

(iv→) l'astensione dall'instaurare il rapporto continuativo, eseguire operazioni o prestazioni professionali, mettendo fine al rapporto continuativo o alla prestazione professionale già in essere di cui siano, direttamente o indirettamente, parte società fiduciarie, trust, società anonime o controllate attraverso azioni al portatore aventi sede in Paesi terzi ad alto rischio. Tali misure si applicano anche nei confronti delle ulteriori entità giuridiche, altrimenti denominate, aventi sede nei suddetti Paesi, di cui non è possibile identificare il titolare effettivo né verificarne l'identità.

In tali casi non potranno essere eseguite operazioni ovvero si dovrà porre fine al rapporto continuativo o alla prestazione già in essere e, fermo l'obbligo di documentare i motivi di mancato perfezionamento o risoluzione del rapporto, si dovrà valutare se effettuare una segnalazione alla UIF (cosiddetto "**Obbligo di astensione**").

L'obbligo di astensione sussiste anche nel caso in cui siano individuate ipotesi di "alto rischio" e indizi di grave o materiale sospetto di una connessione tra l'operazione ed i fenomeni di riciclaggio e finanziamento del terrorismo per i quali l'esecuzione comporti di fatto il perfezionamento, anche nella forma di agevolazione, del reato (che consiste anche nel trasferimento). Tale obbligo sussiste anche per le operazioni di liquidazione poiché i capitali non sarebbero più sottoponibili a sequestro presso la Compagnia; in questo caso, oltre all'astensione, si procederà all'invio di una segnalazione di operazione sospetta alla UIF, anche anticipata da una richiesta (*ex* art. 6 co. 4 D. Lgs. n. 231/07) di "sospensione cautelare" dell'operazione.

[27] Tuttavia, per quanto riguarda i clienti esistenti, il sistema di rating consente di attribuire un livello di rischio elevato alle persone fisiche o giuridiche recentemente sottoposte a sanzione, fino a quando il rapporto d'affari non venga chiuso. Nell'attesa che la chiusura diventi effettiva, l'attività sul contratto di assicurazione sulla vita o di capitalizzazione deve essere bloccata o comunque sottoposta a restrizioni.

[28] La Compagnia, con riferimento alla clientela acquisita tramite intermediari non di Gruppo adotta un approccio restrittivo rispetto ai soggetti con cittadinanza/nazionalità in Paesi MSC, a prescindere dalla residenza.

[29] Si veda la lista dei Paesi "MSC" tempo per tempo vigente.

[30] Si confronti la definizione presente all'interno del paragrafo XI "Acronimi/definizioni".

6. Monitoraggio delle transazioni

Nel corso del rapporto continuativo andrà ad essere effettuato un **controllo costante dell'operatività posta in essere** dalla clientela, volto a **individuare tempestivamente e con efficacia eventuali elementi di incongruenza** da cui potrebbe scaturire una segnalazione di operazione sospetta.

A tal fine, vengono definiti e aggiornati appositi **indicatori di rischio** necessari per individuare e valutare eventuali profili di sospetto di attività di riciclaggio o finanziamento del terrorismo poste in essere dalla clientela.

La definizione di tali indicatori avviene prendendo in considerazione, oltre agli scenari di operazione sospetta stabiliti dal Gruppo[31], anche gli **indicatori di anomalia forniti da Banca d'Italia** nel "**Provvedimento recante gli indicatori di anomalia per gli intermediari**", gli "**Schemi di anomalia UIF**" e/o ogni altro "evento di rischio" individuato dalle "**Linee Guida EBA-ESMA ed EIOPA**" e/o definito, a livello di integrazione dei precedenti e/o quale risultanza dei controlli e/o delle verifiche da parte della Funzione Antiriciclaggio (anche a seguito di ogni, eventuale, interazione e/o conseguenza di attività ispettive dell'Autorità di Vigilanza di settore).

Tali indicatori sono implementati negli strumenti informatici di supporto all'operatività (cfr. "Piattaforma KYC"), i quali generano appositi ***alerts* delle operazioni potenzialmente sospette**. La Compagnia utilizza i criteri e le soglie di rilevanza per l'estrazione delle operazioni/transazioni in base alla propria attività (tipologia dei prodotti assicurativi), alla tipologia della clientela, nonché ai canali di distribuzione ed alla classificazione dei rischi di riciclaggio.

L'attività di gestione degli *alerts*, dall'evenienza delle transazioni potenzialmente anomale, sino alla fase conclusiva di follow up a valere sulle operazioni sospette oggetto di segnalazione, costituisce il processo di ***Alert Management***.

La Procedura di Gruppo CPL0287 "AML/CTF Transaction Monitoring Alert Management Procedure" (recepita a livello locale) definisce, tra gli altri, una serie di principi fondamentali e di *standards* relativi a tale processo, che debbono essere declinati in requisiti operativi minimi da adottare a ciascun livello di analisi, tra cui:

- **Prioritization**, intesa come l'insieme di regole generali secondo cui le attività di analisi/indagine a valere sugli *alerts* devono essere effettuate sulla base della rischiosità dei medesimi *alert*, al fine di garantire la tempestività di indagine di quelli che risultano associati ad operazioni considerate più rischiose (c.d. prioritizzazione);
- **Allocation**, definisce regole di allocazione tra le risorse incaricate dell'analisi di *alert* e casi di indagine, al fine di consentire una visione d'insieme maggiormente obiettiva ed un risultato il più possibile oggettivo e completo.

È prevista, inoltre, un'attività di revisione periodica degli indicatori al fine di limitare i falsi positivi e potersi pertanto concentrare sull'analisi delle situazioni potenzialmente a maggiori rischio, nonché per valutare la necessità di inserire nuovi indicatori individuati sulla base dell'attività condotta, o emergenti a seguito di novità regolamentari, richieste da parte del Gruppo o dal Regolatore.

7. Gestione delle operazioni sospette

È disposto che si provveda a **inviare alla UIF <u>prima del compimento dell'operazione</u> una segnalazione di operazione sospetta** quando si sappia, si sospetti o vi siano motivi ragionevoli per sospettare che siano in corso o siano state compiute o tentate operazioni di riciclaggio o di finanziamento al terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano da attività criminosa.

Il sospetto si fonda su una **valutazione compiuta di tutti gli elementi oggettivi e soggettivi** delle operazioni.

In particolare, il sospetto è desunto da **caratteristiche**, **entità** e **natura dell'operazione**, nonché dal loro collegamento o frazionamento o da qualsiasi altra circostanza conosciuta in ragione delle funzioni esercitate, tenuto

[31] Si confronti paragrafo 4.3. della INS-CPL-FS01 v.11 Global AML-CTF Policy.

conto anche della capacità economica e dell'attività svolta dal soggetto cui è riferita, in base agli elementi a disposizione acquisiti nell'ambito dell'attività svolta.

Nell'ambito dell'attività di collocamento di prodotti assicurativi, l'Intermediario è chiamato ed obbligato (oltre che ai sensi di Legge anche per precise disposizioni contrattuali/istruzioni tempo per tempo predisposte) a segnalare alla Compagnia eventuali casistiche in cui, attraverso i propri canali distributivi, rilevi o venga a conoscenza di un sospetto di riciclaggio e/o finanziamento del terrorismo correlato alla richiesta di apertura di un rapporto/ esecuzione di un'operazione. In particolare, conformemente a quanto disposto dal Provv. IVASS 111/2021, la Compagnia promuove l'applicazione di processi rafforzati di scambio informativo e segnaletico con gli intermediari sia infragruppo sia esterni; a tal fine principi che regolano tali processi sono anche formalizzati all'interno degli accordi distributivi in vigore tra la Compagnia e i partner. Poiché la **segnalazione deve essere effettuata sempre prima del compimento dell'operazione**, in presenza degli elementi di sospetto, è disposto che l'**operazione non debba essere compiuta fino al momento in cui non si sia provveduto ad effettuare la segnalazione**.

La norma fa salvi i casi in cui l'operazione debba essere eseguita ma, in tal caso, ai fini dell'eseguibilità ne deve essere fornita specifica evidenza dell'obbligo di legge per la determinazione finale rimessa alla Funzione Antiriciclaggio, nonché i casi in cui l'esecuzione dell'operazione non possa essere rinviata tenuto conto della normale operatività, ovvero i casi in cui il differimento dell'operazione possa ostacolare le indagini. In questi casi, dopo aver ricevuto l'atto o eseguito l'operazione, si procede ad informare immediatamente la UIF.

Ai sensi dell'art. 6 comma 4 lett. c) del D. Lgs. n. 231/2007 l'UIF, avvalendosi delle informazioni raccolte nello svolgimento della propria attività, può sospendere, anche su richiesta del Nucleo Speciale di Polizia Valutaria della Guardia di Finanza, della D.I.A. e dell'Autorità Giudiziaria, per un massimo di n. 5 giorni lavorativi, sempre che ciò non pregiudichi il corso delle indagini, operazioni sospette di riciclaggio o di finanziamento del terrorismo, dandone immediata notizia a tali Organi.

La **rilevazione dell'operazione sospetta** può avvenire attraverso i seguenti **canali**:

- **Alert provenienti dal Tool di rilevazione delle operazioni sospette** che mediante delle estrazioni informatiche periodiche rileva tutte le potenziali anomalie che dovranno essere oggetto di analisi in **applicazione degli indicatori di anomalia** per gli intermediari finanziari, **rilasciati da Banca di Italia** (Automated Alert) ("Piattaforma KYC")**;**
- **Unusual Activity Reports**:
    - Segnalazione interna / Whistleblowing antiriciclaggio;
    - Profili di rischio alti elaborati dalla Piattaforma KYC;
    - Riscontro positivo con un nominativo presente nelle Liste di controllo;
    - Anomalie rinvenute nell'ambito dello svolgimento dell'adeguata verifica rafforzata (analisi del dossier KYC);
    - segnalazioni provenienti dalla "Rete Distributiva Diretta" nell'ambito dell'assolvimento della "collaborazione attiva" a livello sinergico sugli "stessi clienti" e/o sulle "stesse operazioni" così come definite dal Provv. IVASS n. 111/2021 (in modifica integrativa del Reg. IVASS n. 44/2019).
- **External Triggers**:
    - Segnalazione proveniente dagli Organi di controllo della Compagnia e del Gruppo (Ispezione Generale, Organismo di Vigilanza ai sensi del Dlgs 231/01, Collegio Sindacale);
    - Segnalazione proveniente dalle Autorità (ad es. Magistratura; Guardia di Finanza ecc.) esterne, attraverso la notifica di provvedimenti di indagine e/o di attuazione di sequestri.

La rilevazione di un'operazione sospetta è il risultato di un **processo[32] di analisi complesso**, che prevede il coinvolgimento:

- della funzione Regulatory Controls che ha la responsabilità di effettuare le analisi di I livello sugli *alert*;
- del Delegato alla segnalazione delle operazioni sospette **(Delegato SOS)**, che gestisce il processo di valutazione delle segnalazioni pervenute e la trasmissione delle segnalazioni all'UIF, nonché il flusso delle eventuali richieste di approfondimento provenienti dall'UIF stessa. Tale valutazione segnaletica deve raccordarsi con le determinazioni del Responsabile della Funzione AML in rapporto al livello di rischio individuato e segnalato ed

[32] Per dettagli sul processo cfr. Procedura CAN 01-04-01 "Operazioni sospette di riciclaggio e/o connesse al terrorismo"; e il Manuale Operativo "CAN 01-04-02 Attività da eseguire per le segnalazioni in caso di operazioni sospette_2522367"

anche contemplare, sempre in ragione del rischio, l'eventuale effettuazione di una "segnalazione cautelare" per l'adozione dei provvedimenti urgenti (cfr. art. 6 co. 4 D. Lgs. cit.);

(anche) per ogni necessaria attività di supporto (comprese quelle di natura istruttoria) e di coordinamento, nonché di raccordo con la profilatura del rischio e aggiornamento delle misure di verifica,

- della **Funzione Antiriciclaggio,** che effettua i controlli di II livello per verificare la correttezza delle archiviazioni del primo livello, monitora le posizioni maggiormente rischiose per le quali il I livello ritiene di non avere elementi per poter decidere in autonomia sull'archiviazione della posizione e supporta il Delegato SOS nella fase di istruttoria delle operazioni potenzialmente sospette.

La segnalazione può essere attuata in ogni momento del rapporto ivi compresa la fase di instaurazione dello stesso.

In ordine all'identità delle persone intervenute nell'iter di segnalazione deve essere **garantita la massima riservatezza e confidenzialità**, diretta ad evitare possibili effetti ritorsivi nei loro confronti. Inoltre, è fatto **divieto** ai soggetti tenuti alla segnalazione di operazione sospetta e a chiunque ne sia comunque a conoscenza, **di dare comunicazione al cliente interessato o a terzi dell'avvenuta segnalazione**, dell'invio di ulteriori informazioni richieste dalla UIF o dell'esistenza ovvero della probabilità di indagini e di approfondimenti in materia di riciclaggio o di finanziamento del terrorismo. Tale divieto:

- non si estende alla comunicazione effettuata alle Autorità di Vigilanza di settore in occasione dell'esercizio delle relative attribuzioni;

- non impedisce la comunicazione tra intermediari bancari e finanziari anche nei casi relativi allo stesso cliente o alla stessa operazione che coinvolga due o più intermediari. Le informazioni scambiate possono essere utilizzate esclusivamente ai fini di prevenzione del riciclaggio o del finanziamento del terrorismo.

La segnalazione è dovuta anche in caso di applicazione delle misure restrittive dell'operatività internazionale. In tal caso, ferma la valutazione e segnalazione in conformità alle modalità regolamentari, andrà sempre effettuata una valutazione per contribuire una segnalazione ex art. 35 D. Lgs. n. 231/07.

A seguito della segnalazione di un'operazione sospetta, la Compagnia deve valutare, in sede di Comitato Antiriciclaggio, le adeguate misure da implementare, nel rispetto della normativa vigente, nei confronti di un cliente/partner oggetto di tale segnalazione, al fine di "prendere le distanze" da esso e, in un'ottica di valutazione e contenimento del rischio, al fine di ponderare e diminuire – ove possibile - il rischio inerente.

La decisione di procedere alla segnalazione di operazione sospetta obbliga la Compagnia a valutare l'opportunità di proseguire la relazione ovvero di procedere alla sua chiusura. Si precisa che la decisione di mantenere la relazione comporta la necessità di garantire un'attività di monitoraggio di tipo rafforzato.

8. Contrasto al finanziamento del terrorismo

Al fine di dare esecuzione alle **misure di congelamento di fondi e risorse economiche**[33] stabilite dalle risoluzioni adottate, ai sensi della Carta delle Nazioni Unite dal Consiglio di Sicurezza delle Nazioni Unite, per contrastare e reprimere il finanziamento del terrorismo, il finanziamento della proliferazione delle armi di distruzione di massa e l'attività di Paesi che minacciano la pace e la sicurezza internazionale, qualora Cardif Vita S.p.A. individui un'**operazione sospetta riconducibile ad un'attività di finanziamento del terrorismo**, ovvero dalle attività di esecuzione del **customer screening** emerga un **match accertato con soggetti riconducibili ad attività di finanziamento del terrorismo**, il Delegato SOS **comunica alla UIF** al verificarsi di tali eventi:

- le **misure di congelamento dei fondi applicate** ai soggetti designati nelle liste comunitarie o nei decreti ministeriali, indicando i nominativi coinvolti, l'ammontare e la natura dei fondi;

[33] In base all'art. 1, comma 1, lettera f), punto 9) del D. Lgs. n. 109/2007, le polizze assicurative concernenti i rami vita di cui all'articolo 2, comma 1, del decreto legislativo 7 settembre 2005, n. 209 (Codice delle assicurazioni private) rientrano nella definizione di "fondi".

- le **operazioni**, i **rapporti** e **ogni altra informazione disponibile**, **riconducibile ai soggetti** designati nelle liste, nonché ai soggetti in via di designazione, sulla base di informazioni fornite dalla UIF stessa su indicazione del Comitato di Sicurezza Finanziaria.

Inoltre, in conformità a quanto previsto dal Regolamento (CE) 2580/2001 (articolo 2, paragrafo 1 ed articolo 4) Cardif Vita S.p.A.:

- **congela tutti i capitali e le altre attività finanziarie** di cui ne detenga la proprietà o il possesso una persona fisica o giuridica, gruppo o entità che commettono o tentano di commettere atti terroristici, che partecipano alla loro esecuzione o che la facilitano;
- **prevede il divieto di mettere**, direttamente o indirettamente, **a disposizione** delle persone fisiche o giuridiche, gruppo o entità di cui al punto precedente, capitali e altre attività finanziarie;
- **fornisce**, laddove opportuno, immediatamente tutte **le informazioni atte ad agevolare l'osservanza del Regolamento 2580/2001**, quali gli importi congelati e le operazioni eseguite al **Comitato di Sicurezza Finanziaria presso il MEF** e alla Commissione Europea tramite lo stesso Comitato;
- **collabora con le autorità competenti** di cui al punto precedente per verificare le informazioni fornite.

9. Obbligo di conservazione di documenti, dati ed informazioni

È disposto l'obbligo di **conservare i documenti (direttamente o per il tramite dell'Intermediario Assicurativo), i dati e le informazioni utili** a prevenire, individuare o accertare eventuali attività di riciclaggio o di finanziamento del terrorismo e a consentire lo svolgimento delle analisi effettuate, nell'ambito delle rispettive attribuzioni, dalla UIF o da altra Autorità competente.

Per tali finalità, si deve procedere a conservare **copia dei documenti acquisiti in occasione dell'adeguata verifica della clientela** e **l'originale, ovvero copia avente efficacia probatoria ai sensi della normativa vigente, delle scritture e registrazioni inerenti alle operazioni**. La documentazione conservata deve **consentire**, quanto meno, **di ricostruire univocamente**:

- la **data di instaurazione del rapporto** continuativo (e le analisi preliminari effettuate a supporto della valutazione di congruità e adeguatezza del Cliente);
- i **dati identificativi** del cliente, del titolare effettivo e dell'esecutore e le **informazioni sullo scopo e la natura** del rapporto o della prestazione (in assolvimento della adeguata verifica);
- la **data**, l'**importo** e la **causale dell'operazione**;
- i **mezzi di pagamento** utilizzati.

Con riferimento alla conservazione dei dati, viene disposto di utilizzare i mezzi di conservazione stabiliti, tempo per tempo dalla normativa applicabile, tra i quali **anche gli archivi standardizzati e l'Archivio Unico Informatico** (**AUI**), gestito dall'Ufficio Regulatory Controls, quale sistema che, in attesa dei regolamenti attuativi dell'obbligo (ad emanarsi dall'IVASS) consente di rispettare i requisiti indicati dal Decreto antiriciclaggio.

Il sistema di conservazione e le relative regole, modalità di adeguamento alla normativa - tempo per tempo – vigente, è sotto l'egida del Responsabile della Funzione Antiriciclaggio che può suggerire ogni modifica motivata e/o sostitutiva in adeguamento anche per le finalità di controllo, la verifica ed il mantenimento dell'evidenza documentale. Nel caso si rendano necessarie modifiche sostanziali dei criteri di conservazione dei dati antiriciclaggio e delle correlate informazioni rilevanti, conformemente a qualsiasi modifica che sia inerente ai criteri di redazione della contabilità (in tal caso per finalità di contrasto del riciclaggio e del finanziamento del terrorismo) il Responsabile della Funzione Antiriciclaggio effettuerà una apposita proposta, specificatamente indicando i razionali e ogni utile elemento che renda necessaria e/o utile la modifica, al fine di consentire la valutazione del Consiglio di Amministrazione che provvederà mediante delibera motivata.

Il sistema di conservazione deve:

- permettere di **prevenire qualsiasi perdita di dati ed informazioni** e risultare idoneo a **garantire la ricostruzione dell'operatività o attività del cliente**;

- assicurare l'**accessibilità completa e tempestiva ai dati e alle informazioni** da parte delle Autorità, la **tempestiva acquisizione** dei dati e delle informazioni, con indicazione della relativa data, l'**integrità** dei dati e delle informazioni e la **non alterabilità** dei medesimi successivamente alla loro acquisizione, la **trasparenza**, la **completezza** e la **chiarezza** dei dati e delle informazioni, nonché il mantenimento della **storicità** dei medesimi.

I documenti, i dati e le informazioni acquisiti sono **conservati per un periodo di 10 anni dalla cessazione del rapporto continuativo.**

La Compagnia, a fronte delle novità introdotte dal Decreto n. 55 del MEF, monitora nel complesso il processo di assolvimento degli obblighi di conservazione ed anche provvede a segnalare al Registro di titolarità effettiva (anche il "Registro" – a partire dalla data di effettiva operatività dello stesso) le eventuali incongruenze rilevate tra le informazioni relative alla titolarità effettiva, consultabili nel predetto Registro e le informazioni, relative alla titolarità effettiva, acquisite dai predetti soggetti nello svolgimento delle attività finalizzate all'adeguata verifica della clientela.

Costituisce obbligo della Compagnia provvedere all'**invio mensile alla UIF dei dati aggregati** concernenti la propria operatività nelle modalità e secondo le cadenze stabilite dalla UIF, al fine di consentire l'effettuazione di analisi mirate a far emergere eventuali fenomeni di riciclaggio o di finanziamento del terrorismo (cfr. art. 33 del D. Lgs. 231/2007 e dell'articolo 14, comma 2, lettera g) del Regolamento IVASS n. 44). A corredo dell'obbligo, costituisce anche diligente assolvimento l'analisi immediata di eventuali richieste ricevute dall'UIF circa la segnalazione di potenziali "anomalie statistiche".

10. Formazione

La **formazione del personale sugli obblighi e sulle connesse responsabilità previsti dalla normativa antiriciclaggio**, è curata con carattere di continuità e mediante specifica declinazione per compiti, funzioni e con accertamento della comprensione. Tale formazione non è rivolta ad unità specifiche, ma riguarda tutto il personale della Compagnia.

Per quanto concerne l'erogazione della formazione in ambito antiriciclaggio e di contrasto al finanziamento del terrorismo, la stessa è rivolta a:

- tutti i dipendenti, con contratto a tempo indeterminato/ determinato, di somministrazione e gli stagisti;
- il personale distaccato presso la Compagnia proveniente da società estere del Gruppo (cc.dd. "espatriati IN");
- il personale distaccato presso la Compagnia proveniente da società italiane del Gruppo (cc.dd. "distaccati IN ").

da parte della Compagnia, particolare attenzione viene posta al personale che è a più diretto contatto con la clientela, tenendo conto dell'evoluzione della normativa, delle procedure interne delle imprese nonché delle istruzioni, degli schemi e degli indicatori emanati dalla UIF.

La Funzione Compliance, in cui è integrata la Funzione Antiriciclaggio, partecipa alla redazione del Piano di Formazione aziendale in collaborazione con Human Resources. Il piano, che comprende anche le tematiche antiriciclaggio, viene approvato dal Consiglio di Amministrazione.

Tale Piano prevede il dettaglio delle tipologie di formazione e le relative modalità e tempi di erogazione e di fruizione.
In particolare, la formazione in materia di Compliance e Sicurezza Finanziaria viene erogata con modalità, strumenti e tempistiche differenti, a seconda dei seguenti "*target*" di segmentazione del Personale:

- **nuovi assunti** - formazione "Standard", erogata attraverso sessioni di e-learning e in "aula" anche in modalità virtuale;
- **tutto il personale in organico** - formazioni "Tematiche" erogate attraverso sessioni di e-learning su particolari tematiche di Compliance e Sicurezza Finanziaria previste da Policy e Procedure di Gruppo;

- **personale assegnato a determinate attività aziendali** - per l'esercizio delle quali necessita di formazioni "Specialistiche" in forma di "workshop", erogate sia in aula sia in modalità e-learning dalla Funzione Compliance medesima o da consulenti esterni, esperti in materia;
- **personale della Funzione Antiriciclaggio**.

In particolare, si precisa che nell'ambito del programma di addestramento e formazione della Funzione Antiriciclaggio, oltre ai corsi derivanti da obblighi formativi interni ed esterni, la stessa Funzione usufruisce nel corso dell'anno anche degli ulteriori corsi di tipo manageriale, comportamentale e tecnico finalizzati al rafforzamento delle relative competenze specifiche richieste dall'attività svolta.

L'erogazione di detta formazione al Personale avviene sia mediante l'utilizzo di **corsi "e-learning"** fruibili sulla piattaforma di Gruppo "My Development", sia attraverso delle apposite **sessioni formative "in aula"**, tenute dalla Funzione Antiriciclaggio o da consulenti esterni specialisti delle materie oggetto di formazione. Sono previsti **programmi specifici** per il **personale della Funzione Antiriciclaggio** così da garantirne il continuo aggiornamento in merito all'evoluzione del rischio di riciclaggio, nonché agli schemi tipici delle operazioni finanziarie criminali.

Per l'area tematica antiriciclaggio e contrasto al finanziamento del terrorismo sono stati individuati i seguenti argomenti sensibili e i relativi *target group*:

- Nuovi assunti

Entro 30 giorni dall'assegnazione del corso, che interviene non oltre il mese successivo all'assunzione, il personale neoassunto ha l'obbligo di effettuare una serie di corsi di formazione, in modalità *e-learning*, tra cui i seguenti in materia di antiriciclaggio e Sicurezza Finanziaria che hanno l'obiettivo di illustrare i principi generali e di carattere normativo:

- "Lotta al riciclaggio di denaro e finanziamento del terrorismo – Nuovi assunti", della durata di 25 minuti;
- "Compliance - Sanzioni finanziarie ed Embarghi - Nuovi assunti", della durata di 45 minuti. Tali corsi prevedono l'obbligo di superamento di un test finale di apprendimento, con rilascio di relativo attestato.

Con riferimento alla formazione in "aula-virtuale" si segnala che il personale neo assunto fruisce, tra gli altri, del corso "Antiriciclaggio e contrasto al finanziamento del terrorismo e altre tematiche legate alla Sicurezza Finanziaria e alla Normativa Fiscale (FATCA e AEOI)". La durata del corso è di 2 ore c.a. e prevede il superamento di un test finale per la valutazione del livello di apprendimento.

- Tutto il personale in organico

Nei confronti del personale in organico vengono rilasciati ogni anno nuovi contenuti di taluni corsi online già presenti sulla piattaforma "MyDevelopment" ed afferenti alle tematiche di Sicurezza Finanziaria. Taluni corsi sono stati attribuiti direttamente dal Gruppo all'intera popolazione aziendale. Per alcuni altri corsi sono previste versioni differenziate del corso a seconda della differente esposizione del personale alla tematica trattata, nonché della posizione ricoperta in azienda.

- Personale assegnato a determinate attività aziendali

Per tutto il personale che necessita, in virtù della propria attività lavorativa, di nozioni formative più specifiche e di approfondimenti in relazione alle tematiche antiriciclaggio o aventi riflesso sulle tematiche di Sicurezza Finanziaria, sono attivati appositi corsi.

- Personale della Funzione Antiriciclaggio

La formazione continuativa delle risorse della Funzione Antiriciclaggio è rivolta sia all'aggiornamento delle necessarie conoscenze normative sia al più generale sviluppo del *know-how* assicurativo e delle competenze manageriali delle stesse. Vengono altresì organizzate delle sessioni di formazione interna, tenute dalle principali funzioni aziendali con cui la Funzione intrattiene maggiori interrelazioni. In tali sessioni le funzioni aziendali coinvolte illustrano alle risorse della Funzione le proprie attività o i progetti che li hanno coinvolti, che sono di interesse per la stessa al fine non solo di ampliare la conoscenza dei processi aziendali, ma altresì di creare efficaci sinergie.

La Funzione Antiriciclaggio, inoltre, aderisce e partecipa costantemente ad eventi esterni quali workshop, seminari e convegni di aggiornamento professionale.

La **rete distributiva diretta** di Cardif Vita è costituita principalmente da intermediari bancari. In particolare nei confronti del principale partner della Compagnia vengono fornite apposite istruzioni operative con riferimento ai

prodotti assicurativi commercializzati e agli obblighi antiriciclaggio. Al riguardo, si specifica che la formazione in materia AML viene erogata anche al personale distaccato di BNL[34].

La Funzione Compliance, anche con riferimento alle tematiche antiriciclaggio, (i) formalizza in specifici report il training fruito dal personale e (ii) **rendiconta sull'attività formativa** nella **relazione annuale** redatta in collaborazione con Human Resources e Global Security e sottoposta all'approvazione del Consiglio di Amministrazione.

11. Acronimi/definizioni

AML	Anti-Money Laundering/ Antiriciclaggio	L'Antiriciclaggio è l'insieme dei presidi a contrasto del rischio di riciclaggio come di seguito definito: - 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; - 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 delittuosa 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 delitto o da una partecipazione allo stesso; - 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.
Conservazione/AUI	Obblighi di Conservazione/ (già) Archivio Unico Informatico	Archivio standardizzato, formato e gestito a mezzo di sistemi informatici, nel quale sono conservati in modo accentrato tutti i dati e le informazioni acquisite nell'adempimento degli obblighi antiriciclaggio.
AuM	Asset under Management	Ammontare del patrimonio gestito.
AEOI	Automatic Exchange of Information (scambio automatico di informazioni)	Scambio di informazioni sui conti finanziari dei non residenti con le autorità fiscali del Paese di residenza dei titolari, per il tramite dell'Agenzia delle Entrate.
AML/CTF - TM	Anti-Money Laundering/ Counter Terrorism Financing - Transaction monitoring (Monitoraggio delle Transazioni ai fini Antiriciclaggio / Contrasto al finanziamento del terrorismo)	Processo mediante il quale vengono identificate, gestite e monitorate le operazioni/transazioni potenzialmente sospette con l'obiettivo di determinare, a seguito delle analisi, se esse debbano essere oggetto di segnalazione all'UIF locale. Tale processo di analisi e di controllo è altresì basato sulla suddivisione dei compiti tra prima e seconda linea di difesa e sulla conseguente definizione di flussi informativi/decisionali.

[34] Alla rete distributiva diretta vengono comunque fornite circolari esterne che descrivono le modalità di utilizzo degli strumenti informatici forniti e le attività che devono essere svolte in materia di adeguata verifica della clientela e segnalazione di operazioni sospette.

BENEFICIARIO		La persona fisica o il soggetto diverso da una persona fisica che, sulla base della designazione effettuata dal contraente o dall'assicurato, ha diritto di percepire la prestazione assicurativa corrisposta dall'impresa di assicurazione; l'eventuale persona fisica o il soggetto diverso da una persona fisica a favore del quale viene pagata la prestazione assicurativa su disposizione del beneficiario designato.
CAC	Comitato Accettazioni Clienti	Comitato avente la finalità di assolvimento delle misure di adeguata verifica rafforzata; in particolare lo scopo del comitato è quello di sottoporre all'Organo con funzione di gestione o ai suoi delegati, al Business unitamente alla Funzione Antiriciclaggio, i rapporti d'affari, nuovi ed esistenti che presentano un livello di rischio "significativo" in termini di riciclaggio, di finanziamento del terrorismo, e mancato rispetto delle sanzioni.
CCIR	Comitato per il Controllo Interno e i Rischi	Comitato endoconsiliare istituito ai sensi del Regolamento IVASS n. 38 del 2018, articolo 6, composto da amministratori non esecutivi in maggioranza indipendenti ai sensi dell'articolo 2387 del codice civile.
CLIENTE		Il soggetto che, anche mediante cointestazione, instaura rapporti continuativi ovvero compie operazioni con la Compagnia.
CSR	Corporate Social Responsability Exclusion List	La CSR Exclusion List, redatta dal Corporale Social Responsibility Department del Gruppo BNP Paribas, che elenca le società e/o i prodotti in riferimento a cui BNP Paribas esclude ogni operatività.
CCRM	Compliance Control, Risk Management	La struttura «Compliance Control, Risk Management» (CCRM) ha il compito di definire controlli e procedure trasversali.
CTF	Counter Terrorism Financing / Lotta Contro il Finanziamento del Terrorismo	Qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione di fondi e risorse economiche, in qualunque modo realizzata, destinati ad essere, direttamente o indirettamente, in tutto o in parte, utilizzati per il compimento di una o più condotte con finalità di terrorismo, secondo quanto previsto dalle leggi penali, ciò indipendentemente dall'effettivo utilizzo dei fondi e delle risorse economiche per la commissione delle condotte anzidette.
COMEX	Comitato Esecutivo	Assicura il coordinamento e la supervisione di tutte le attività operative svolte all'interno della Compagnia.
DATI IDENTIFICATIVI		Dati identificativi del beneficiario, del relativo titolare effettivo e dell'esecutore: - il nome e il cognome, il luogo e la data di nascita; - nel caso di soggetti diversi da persona fisica, la denominazione, la sede legale, il numero di iscrizione nel registro delle imprese ovvero nel registro delle persone giuridiche ove previsto; - in entrambi i casi, al momento della liquidazione della prestazione, anche la residenza anagrafica e, ove diverso, il domicilio, il codice fiscale del beneficiario e, ove ne sia prevista l'assegnazione, anche del relativo titolare effettivo e dell'esecutore.
DECRETO ANTIRICICLAGGIO		Il decreto legislativo 21 novembre 2007, n. 231 e ss. m. e i.
DISPOSIZIONI SULLA CONSERVAZIONE DI DATI E INFORMAZIONI IN ARCHIVI INFORMATIZZATI		Disposizioni specifiche per la conservazione e l'utilizzo dei dati e delle informazioni relativi ai clienti, contenuti in archivi informatizzati, ivi compresi quelli attualmente istituiti presso i soggetti vigilati, che l'IVASS può emanare ai sensi dell'articolo 34, comma 3, del decreto antiriciclaggio.

ESECUTORE		Il soggetto delegato ad operare in nome e per conto del cliente o del beneficiario o il soggetto cui siano conferiti poteri di rappresentanza che gli consentano di operare in nome e per conto del cliente o del beneficiario; ove il soggetto non sia una persona fisica, la persona fisica alla quale in ultima istanza sia attribuito il potere di agire in nome e per conto del cliente.
FATCA	Foreign Account Tax Compliance Act/ Legge sulla conformità fiscale dei conti esteri	Identificazione e comunicazione all'Agenzia delle Entrate dei conti finanziari (comprese le polizze) detenuti da soggetti residenti o cittadini degli Stati Uniti.
FATF/ GAFI	Financial Action Task Force/ Gruppo di Azione Finanziaria Internazionale	Organismo intergovernativo composto da Stati membri che aderiscono alle raccomandazioni, agli standard globali e al monitoraggio per la lotta al riciclaggio di denaro e al finanziamento del terrorismo.
FUNZIONI FONDAMENTALI	-	Le funzioni di revisione interna, di verifica della conformità, di gestione dei rischi e attuariale di cui all'articolo 30, comma 2, lettera e), del Codice delle Assicurazioni Private.
MEZZI DI PAGAMENTO	-	Mezzi di pagamento di cui all'articolo 1, comma 2, lettera s), del decreto antiriciclaggio
MISURE RAFFORZATE	-	Obblighi di adeguata verifica della clientela di cui agli articoli 24 e 25 del decreto antiriciclaggio
MISURE SEMPLIFICATE	-	Gli obblighi di adeguata verifica della clientela di cui all'articolo 23 del decreto antiriciclaggio
IVASS	Istituto per la Vigilanza sulle Assicurazioni	Autorità di Vigilanza nei confronti delle Imprese di Assicurazioni
HS (Paesi)	High sensitive Countries/ Paesi ad Alta sensibilità	Paesi classificati ad alta sensibilità dal Gruppo BNP Paribas sulla base sia (i) di criteri esterni basati su indicatori pubblicati da organizzazioni internazionali che fungono da guida e valutazione di fenomeni di finanziamento del terrorismo, corruzione, riciclaggio di denaro, paradisi fiscali, sanzioni erogate direttamente agli Stati e violazione di diritti umani, che (ii) di criteri interni di BNP Paribas che consentono la valutazione del livello di sicurezza finanziaria connesso alla fornitura di servizi finanziari e bancari in tali Paesi.
KYC	Know Your Customer/ Adeguata verifica della clientela	L'adeguata verifica della clientela comprende i) l'identificazione e la verifica dell'identità del cliente e delle altre parti rilevanti del contratto quali esecutore, titolari effettivi, terzi pagatori (ove richiesto) e terzo percipiente, nonché ii) l'ottenimento di informazioni sullo scopo e sulla natura del rapporto instaurato o dell'operazione occasionale, ed infine iii) l'esecuzione del controllo costante del rapporto con il cliente, per tutta la sua durata.
KYI	Know Your Intermediary – Conoscenza dell'intermediario	Standard di due diligence per l'identificazione e la valutazione degli intermediari con cui la Compagnia entra in relazione d'affari
MSC	Major Sanctioned Countries	Paesi e Regioni soggetti a sanzioni globali imposte dall'OFAC (Office of Foreign Assets Control) ovvero Paesi e Regioni ad alto rischio nei confronti dei quali BNPP ha deciso di mantenere le medesime misure restrittive di controllo. Le sanzioni globali imposte dall'OFAC riguardano attualmente i seguenti Paesi: Cuba, Corea del Nord, Iran, Siria e la Regione Ucraina Crimea/Sebastopoli.
OPERAZIONE	-	Impiego dei mezzi di pagamento.
ORGANO CON FUNZIONE DI GESTIONE (per l'Antiriciclaggio)		L'Amministratore Delegato cui sono demandati compiti di verifica dell'esecuzione dei piani di intervento AML e CTF deliberati dal Consiglio di Amministrazione con poteri e facoltà di (i) designazione dei singoli dirigenti specificamente delegati alla realizzazione di ciascun intervento e per il monitoraggio di "prossimità" e tecnico delle attività da eseguirsi; (ii) adeguamento alla normativa e agli orientamenti, tempo per tempo, emanati dalle Autorità. Ha facoltà di non accogliere eventuali proposte di interventi organizzativi e procedurali presentate

		dal responsabile della funzione antiriciclaggio previa formalizzazione delle motivazioni della decisione.
ORIENTAMENTI	-	Orientamenti congiunti, indirizzati alle autorità competenti degli Stati membri delal unione Europea (UE), nonché agli intermediari bancari e agli intermediari finanziari, emanati dalle Autorità Europee di Vigilanza (AEV) ai sensi degli articoli 17, 18 e 48 della Direttiva (UE) 2015/849 del 20 maggio 2015.
PEPs	Persone politicamente esposte	Art. 1 c.2 lettera. dd) del D. Lgs.231/2007 e ss. m. e i.: persone fisiche che occupano o hanno cessato di occupare da meno di un anno importanti cariche pubbliche, nonché i loro familiari e coloro che con i predetti soggetti intrattengono notoriamente stretti legami.
PERCIPIENTE	-	L'eventuale persona fisica o il soggetto diverso da una persona fisica a favore del quale viene pagata la prestazione assicurativa su disposizione del beneficiario designato.
PIL	Politici Italiani Locali/Persone Localmente Importanti	Sono soggetti che non sono classificati da una apposita definizione del Decreto e vengono ricompresi nell'ambito della categoria PEPs, a seguito di valutazione da parte della Funzione Antiriciclaggio, in quanto ritenuto accomunati dal medesimo rischio, in conformità agli Orientamenti.
RAPPORTO CONTINUATIVO	-	Un contratto individuale di assicurazione rientrante nei rami di cui all'articolo 2, comma 1, del Codice, incluse le "singole applicazioni" di una "convenzione", o un "contratto di assicurazione" concluso mediante la sottoscrizione del documento – comunque denominato dalle parti nell'ambito di un contratto collettivo di assicurazione, rientrante nei rami di cui all'articolo 2, comma 1, del Codice – che comporta l'inclusione di una "singola posizione" nella copertura assicurativa di tale contratto collettivo, in conformità con le definizioni di "singole posizioni" incluse nella copertura dei "contratti collettivi" e di "singole applicazioni" delle "convenzioni", di cui all'articolo 7, comma 1, del regolamento ISVAP n. 27 del 14 ottobre 2008 concernente la tenuta dei registri assicurativi.
REGISTRO DEI TITOLARI EFFETTIVI/ REGISTRO DI TITOLARITA' EFFETTIVA		Registro istituito presso la Camera di Commercio (sezione speciale) in conformità al Decreto del Ministero dell'Economia e delle Finanze concernente i dati dei "titolari effettivi" dei soggetti differenti da persone fisiche.
RETE DISTRIBUTIVA DIRETTA	-	Le persone fisiche o le società - iscritte nel registro unico elettronico degli intermediari assicurativi di cui all'articolo 109, comma 2, lettere a), c) e d), del Codice, ovvero gli omologhi soggetti annotati nell'elenco annesso al registro a seguito della notifica di cui agli articoli 116-quater e 116-quinquies del Codice - che distribuiscono prodotti assicurativi nei rami di attività elencati all'articolo 2, comma 1 del medesimo Codice.
RISCHIO DI RICICLAGGIO	-	Il rischio derivante dalla violazione di previsioni di legge, regolamentari e di autoregolamentazione funzionali alla prevenzione dell'utilizzo del sistema finanziario per finalità di riciclaggio, di finanziamento del terrorismo e di finanziamento dei programmi di proliferazione delle armi di distruzione di massa, nonché di coinvolgimento in episodi della stessa specie.
SOS	Segnalazione di Operazioni Sospette	I soggetti obbligati, prima di compiere l'operazione, inviano senza ritardo alla UIF, una segnalazione di operazione sospetta quando sanno, sospettano o hanno motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo o che comunque i fondi,

		indipendentemente dalla loro entità, provengano da attività criminosa.
TERZO PAGATORE	-	Soggetto diverso dal contraente che, anche senza essere dotato di specifico potere rappresentativo o senza fornirne documentazione, effettua il pagamento del premio assicurativo.
TITOLARE EFFETTIVO	-	È considerato "titolare effettivo": - la persona fisica o le persone fisiche per conto delle quali il cliente instaura un rapporto continuativo o realizza un'operazione (in breve, "titolare effettivo sub 1"); - nel caso in cui il cliente o il soggetto per conto del quale il cliente instaura un rapporto continuativo o realizza un'operazione siano soggetti diversi da una persona fisica, la persona o le persone fisiche cui, in ultima istanza, è attribuibile direttamente o indirettamente la proprietà di tali soggetti ovvero il relativo controllo (in breve, "titolare effettivo sub 2"), - la persona o le persone fisiche cui, in ultima istanza, è attribuibile direttamente o indirettamente la proprietà ovvero il relativo controllo del soggetto, diverso da una persona fisica che ha diritto di percepire la prestazione assicurativa, sulla base della designazione effettuata dal contraente o dall'assicurato, o a favore del quale viene effettuato il pagamento, su eventuale disposizione del beneficiario designato (in breve, "titolare effettivo sub 3"); - i criteri di cui agli articoli 20 e 22, comma 5, del decreto antiriciclaggio, in quanto compatibili, si applicano per individuare il titolare effettivo anche nei casi in cui il cliente o il soggetto per conto del quale il cliente instaura un rapporto continuativo o effettua un'operazione oppure il beneficiario siano: - i. società, anche di persone, - ii. altri soggetti giuridici privati, anche se con sede all'estero, - iii. trust espressi, indipendentemente dal relativo luogo di istituzione e dalla legge ad essi applicabile
UIF	Unità di Informazione Finanziaria	L'UIF, nel sistema di prevenzione del riciclaggio e del finanziamento del terrorismo, è l'Autorità incaricata di acquisire i flussi finanziari e le informazioni riguardanti ipotesi di riciclaggio e di finanziamento del terrorismo principalmente attraverso le segnalazioni di operazioni sospette trasmesse da intermediari finanziari, professionisti e altri operatori; di dette informazioni effettua l'analisi finanziaria, utilizzando l'insieme delle fonti e dei poteri di cui dispone, e valuta la rilevanza ai fini della trasmissione agli organi investigativi e della collaborazione con l'Autorità giudiziaria, per l'eventuale sviluppo dell'azione di repressione.
VHS Countries	Very High Sensitive Countries / Paesi ad altissima sensibilità	Paesi classificati ad altissima sensibilità dal Gruppo BNP Paribas sulla base sia (i) di criteri esterni basati su indicatori pubblicati da organizzazioni internazionali che fungono da guida e valutazione di fenomeni di finanziamento del terrorismo, corruzione, riciclaggio di denaro, paradisi fiscali, sanzioni erogate direttamente agli Stati e violazione di diritti umani, che (ii) di criteri interni di BNP Paribas che consentono la valutazione del livello di sicurezza finanziaria connesso alla fornitura di servizi finanziari e bancari in tali Paesi.

12. Allegato 1 - INS-CPL-FS01-V11 Cardif Global AML CTF Policy

Global Anti Money Laundering and Counter-Terrorist Financing (AML-CTF) Policy

Issuer (owner entity)*	100 013 - Compliance			
Process(es) Involved*	PR00005 - Compliance			Others *Please specify*
Risk(s) Involved*	L1-RIT0001 Compliance / L2-RIT0024 Financial Security - AML (Anti Money Laundering) related risk	L1-RIT0001 Compliance / L2-RIT0019 Financial Security - International Sanctions and Embargoes related risk	L1-RIT0001 Compliance / L2-RIT0018 Financial Security - Anti-bribery & Corruption related risk	Others *Please specify*
Keywords	AML-CTF, Group Supervision, Risk Classification, KYC, Transactions Monitoring, Country Sensitivity, Information Sharing, Management Information, Reporting			

Level*	Level 2			
Norm Type*	1- Policy			
Organizational entity Scope of Application*	BNP Paribas Cardif – all entities			
Geographical Scope of Application*	Worldwide	Select an item	Select an item	Others ……
To Adapt Locally*	Applied as such			
Classification rules*	Internal			
Author(s)*	Marco MESCHI			
Author role*	Compliance Cardif			
Validator(s)*	Cardif Compliance Executive Committee			
Sponsor	Karim MOHAMMEDI			

Reference*	INS-CPL-FS01	
Version*	11	
Date of previous version*	28/08/2019	☐ N/A
Validation date*	20/12/2022	
Publication date*	03/01/2023	
Effective date*	04/01/2023	
Renewal date*	20/12/2025	
Implementation deadline*	30/04/2023	

Overarching policy*	Group Compliance Function Charter (DG0018EN)	☐ N/A

	BNP Paribas CARDIF procedure Compliance Governance Principles (INS – CPL – TRANS01)	
Related norms*		
Regulatory text(s) / legal provision(s)	- FATF Recommendations - EU 4th Money Laundering Directive 2015/849 - EU 5th Money Laundering Directive2018/843 amending the 4th Money Laundering Directive - Regulation (EU) 2015/847 on Information Accompanying Transfers of Funds - Ordinance n° 2016-1635 (transposing into French Law the 4th Money Laundering Directive) - Ordinance n° 2020-115 (transposing into French law the 5th Money Laundering Directive) - French Decree n° 2020-118 of 12 February 2020 related to the AML-CTF national framework - French Decree n0 2020-119 of 12 February 2020 related to the AML-CTF national framework - French Decree of 25 February 2021 amending the French Decree of 3 November 2014 (internal control of credit institutions & investment companies) related to the Internal Control of banking, payment services and investment services activities - French Decree of 25 February 2021 amending the French Decree of 6 January 2021 related to the AML/CTF and asset freezing internal control - ACPR Guidelines of 2 March 2020 related to the supervision of AML/TF framework by a Group - Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions - ACPR AML-CTF Guidelines[1] - The French Monetary and financial Code	
Referenced Procedures for BNP Cardif	- INS-CPL-FS04 Procedure related to relationship with PEPs- Savings & protection activities - INS-CPL-FS05 Know Your Intermediary Policy - INS-CPL-FS06 Anti-Corruption Policy - Insurance Business Line - Savings and protection activities - France And international entities - INS-CPL-FS10 Group Procedure on Reporting of Attempts to Circumvent or Evade U.S. Sanctions - INS-CPL-FS13 Group Screening and Recusal Policy for U.S. Persons - INS-CPL-FS14 Investment Solutions Compliance & Control Guidelines for Escalating Material Negative News regarding Network Branches and Affiliates - INS-CPL-FS15 OFAC Voluntary Self-Disclosures Procedure - INS-CPL-FS19 Country policy - INS-CPL-FS20 Sanctions escalation procedure - INS-CPL-FS25 Know Your Client - Global Policy - CPL0253 Know your Client – Segment : Commercial Corporate - CPL0255 Know your Client – Segment : Wealth Management - CPL0257 Know your Client – Segment : Small Businesses - CPL0260 Know your Client – Segment : Private Investment Vehicles - CPL0266 Know your Client – Segment : Retail Markets (Individual Clients only) - CPL0267 Know your Client – Segment : Private Banking - CPL0269 Know your Client – Segment : Nonprofit Private Entities - INS-CPL-FS34 Supplier Knowledge - Financial Security Operational Controls INS-CPL-FS42 procedure Sanctions Advisory Routing and Decision Process for Sanctions & Advisory issues (specifically AD09 - Reinforced decision process for new activities with US Nexus) - INS-CPL-FS35 Global Sanctions Policy - INS-CPL-FS36 Screening of the Relationships - INS-CPL-FS39 Cuba Policy - INS-CPL-FS40 Group procedure concerning the situation in Ukraine and Crimea Sevastopol - Related sanctions - INS-CPL-FS41 - Relationships Involving Individual Nationals and Residents of the Major Sanctioned Countries (and Regions) of Iran, Syria, North Korea and Crimea/Sevastopol - INS-CPL-FS42 procedure Sanctions Advisory Routing and Decision Process for Sanctions & Advisory issues (specifically AD09 - Reinforced decision process for new activities with US Nexus)	

[1]https://acpr.banque-france.fr/controler/lutte-contre-le-blanchiment-des-capitaux-et-le-financement-du-terrorisme/lignes-directrices-principes-dapplication-sectoriels-positions-et-avis (in French only)

	- INS-CPL-FS45 Group policy on Anti Money Laundering and Counter Terrorist Financing trainings - INS-CPL-FS55 AML TM General policy on Anti Money Laundering and Counter Terrorist Financing - Guidelines related to the Asset Freeze (template)
Control plan ref, if any	
Evidence(s)	

Fields required by Compliance

Source*	Regulation / Law & Group standards	
Compliance scoping criteria*	Activity All activities	
	Additional criteria	- Applicable to all entities in the AML-CTF perimeter - (CF Section 1)

Associated documents*	All documents listed in this field are considered as binding

* mandatory field

In this procedure, sections highlighted in orange are added by BNP Paribas Cardif on the previous version already, and in red, the new BNPP Cardif specificities.

In this procedure, sections in red are the new sections not present in the old version

Sections highlighted in grey in a square are not applicable as such to BNP Paribas Cardif.

EXECUTIVE SUMMARY

The Global Anti Money Laundering and Counter Terrorist Financing Policy (the "Global AML-CTF Policy") is the foundation of the Bank's AML-CTF framework. Every BNP Paribas[2] employee is responsible for understanding how the Bank's AML-CTF policies and procedures apply within his or her job responsibilities and for performing his or her duties accordingly. Success in fighting against money laundering ("ML"), terrorist financing ("TF") and the changing face of economic crime depends upon the vigilance of each BNP Paribas employee. That is the driving force behind this policy which contributes to how the Bank effectively prevents, detects and mitigates its ML/TF risks.

As a global financial institution, BNPP, and its subsidiary, BNP Paribas Cardif, is accountable to multiple regulators that stand united around Financial Action Task Force ("FATF") standards to fight money laundering and terrorist financing. This policy reflects the Bank's/BNP Paribas Cardif commitment to act and be recognized as a responsible and trusted business partner, compliant with all applicable regulations, International (e.g., the FATF Recommendations), European (e.g., the European directives (4th and 5th AML directives)) and nationals (e.g., the French Monetary and Financial Code, ACPR guidelines, etc.). In addition, due to its worldwide presence, local regulations apply.

Money laundering is the processing of criminal proceeds to disguise their illegal origin. Corruption, tax crime, drug trafficking, organized crime, embezzlement and other serious offences known as 'predicate offences'[3] generate significant profits that criminals seek to legitimize by changing their form or moving them to another country to cover up their criminal source.

TF remains as one of the Bank's/BNP Paribas Cardif main concerns and refers to the financing of acts of terrorism[4], terrorists and terrorist organizations. TF can be done deliberately and out of conviction (intentional nature) or it can be done through weakness or negligence, or through coercion (e.g. racketeering or kidnappings for ransom). TF can be funded through the use of either illicit or legitimate funds.

Whether it is Micro-Terrorist Financing[5] or Macro-Terrorist Financing[6], the Group is committed to fight terrorism and implement appropriate set up and measures to identify, detect, investigate, and take relevant actions against TF.

---

[2] In the overall procedure BNP Paribas is referred as the Bank, the Group, BNPP or BNP Paribas

[3] FATF Recommendation 3, Interpretive note 3: Predicate offences should include all serious offences or offences punishable by a minimum penalty >1 year imprisonment or for countries with a minimum threshold, a minimum >6 months imprisonment. See FATF list of predicate offences in *Glossary of the FATF Recommendations.*.

[4] There is no international consensus on the definition of "terrorism" but it can nonetheless be defined at the very least by the definition proposed in 2004 by the group of eminent people and the Secretary General of the United Nations as: *"any act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act"*. This definition is the one chosen and used by the Financial Action Task Force ("FATF"), the European Union and the French authorities in their CTF recommendations.

[5] Micro-Terrorist Financing is characterized by acts of terrorism financed mostly by individuals with small amounts, rapid execution, using money transfers, payment services loans, insurance policies, online pot, crowdfunding and takes often place through friends, family and communities.

[6] Macro -Terrorist Financing is the financing of religious, political or military organizations of a terrorist nature on a large scale and over time. The flows are performed in such way that the suspicious flows are hidden behind activities that might seem legal such as business or financial market activities and using collection and/or transfer of funds for philanthropic purposes

To ensure the source and destination of funds and operations, BNP Paribas Cardif entities must comply with these standards.

- ✓ Each BNP Paribas Cardif entity should screen its business relationships against the Group's set of lists, which is managed by the Business Intelligence Unit ("BIU").
- ✓ Receipts and payments must be strictly controlled: the receipt/payment of funds is carried out through an account opened in the customer's name with a credit institution from an EU / EEE country or equivalent third country or country in which the entity is located (for example: Turkey). Cash receipts and payments are prohibited.
- ✓ Measures of assets freezing must be implemented by each BNP Paribas Cardif entity as soon as they enter into force, with accountability for results. This involves setting up an internal organization and procedures for the implementation of asset freezing measures and the prohibition of making available or using funds or economic resources[7].

For further information:

- INS-CPL-FS10 Group Procedure on Reporting of Attempts to Circumvent or Evade U.S. Sanctions
- INS-CPL-FS13 Group Screening and Recusal Policy for U.S. Persons
- INS-CPL-FS15 OFAC Voluntary Self-Disclosures Procedure
- INS-CPL-FS19 Country policy
- INS-CPL-FS35 Global Sanctions Policy
- INS-CPL-FS36 Screening of the Relationships
- INS-CPL-FS39 Cuba Policy
- INS-CPL-FS40 Group Procedure Concerning Ukraine/Russia-related Sectoral Sanctions
- INS-CPL-FS41 - Relationships Involving Individual Nationals and Residents of the Major Sanctioned Countries (and Regions) of Iran, Syria, North Korea and Crimea/Sevastopol
- INS-CPL-FS42 procedure Sanctions Advisory Routing and Decision Process for Sanctions & Advisory issues (specifically AD09 - Reinforced decision process for new activities with US Nexus)
- INS-CPL-FS45 Group policy on Anti Money Laundering and Counter Terrorist Financing trainings
- Guidelines related to the Asset Freeze (template)

To face this increasing underground economy and new technologies that contribute to illicit activities, regulators (international, European, or national) impose a stringent regulatory framework to banks and financial institutions. Noncompliance with the regulations can subject the Bank/ BNP Paribas Cardif to penalties and reputational damage. While the cost associated with monetary penalties is measurable, the reputational cost causes unquantifiable damages that can affect the trust of our clients, business partners and stakeholders. Penalties for ML-TF offences can be severe for the legal entities, board members, Head of AML-CTF framework and even employees, ranging from warnings to fines, loss of a business license for the legal entity, imprisonment, prosecution and cease and desist orders.

[7] Articles L. 562-1 and seq., R. 562-1 and seq. of the French Monetary and Financial Code

WHAT'S NEW?

Principal changes include:

- Section 2 defines the approach to the Group's consolidated supervision
- Section 4.7 introduces the information sharing principle
- Section 4.10 stipulates that relevant metrics should be shared with the appropriate stakeholders in order to highlight areas of high risk and define actions to mitigate them.
- Removal of sections related to Applicability and Exceptions. Section 1 clarifies the scope of applicability

TABLE OF CONTENTS

1 Scope

The Global AML-CTF Policy is applicable to all BNP Paribas entities that belong to the Group AML/CTF perimeter, including BNP Paribas Cardif, whether they are regulated or not.

As a consequence, all entities in Group AML/CTF perimeter must complete and maintain a ML/TF risk classification as described in section 3.

Amongst these entities, the AML-CTF framework described in section 4 must be deployed as follow:

- AML-CTF regulated entities must implement the whole framework
- Non-AML-CTF regulated entities:
    - Identifying a substantial ML/TF risk (medium, high or very high) in their ML/TF risk classification must implement the whole framework
    - Identifying a low ML/TF risk can deploy an adapted framework proportionate to the risks they are exposed to such as the specificity of their activities.

This document must be further deployed as such or transposed as per the Compliance Norm's Management Procedure (CCC0016/ INS-CPL-CCRM06).

2 Group Consolidated Supervision

The scrutiny over money laundering and terrorist financing increases constantly. The globally applied FATF Recommendations aims at strengthening the overall AML-CTF supervision within international Groups such as BNP Paribas. Among others, recommendation 18[8] which relates to the internal control framework significantly reinforces the bank's obligations in terms of Group level oversight.

Consolidated supervision is essential for the Group[9] to identify, monitor and manage the ML-TF risks across the bank, including the ones related to its branches and subsidiaries.

Firstly, a consistent Group consolidated supervision must be based on common AML/CTF standards:

(i) Group AML-CTF procedures based on risks identified in the Group ML-TF risk classification.
(ii) Common rules in terms of identification and assessment of the ML-TF risks at entities level (through the ML/TF risk classification).
(iii) A strong internal control set-up at Group level to assess the Group overall AML-CTF framework's efficiency.

Secondly, an effective Group consolidated supervision includes the monitoring of entities' activities and their ML-TF risks.

To that end, the nature and quality of information gathered from entities must be accurate enough to provide sound indicators so the Group's management and its supervisory body can oversee the ML-TF risks and ensure

[8] Recommendation 18 related to the Internal Control and Group supervision, Article 45 of the EU Anti-money Laundering Directive transposed by Articles L.511-34 and R.561-29 of the French Monetary & Financial Code

[9] Subgroups are subject to the same provisions as for the Group. So are the requirements from Section 3 and 4 which should be adapted based on the subgroup's AML/CTF regulation and its internal organization and governance. Note that Cardif as an Insurance Group also performs its entities supervision including both branches and subsidiaries.

they are effectively mitigated. Indeed, the Group is expected to ensure that its common AML-CTF framework is being deployed appropriately and is effective. Any risk area and/or potential deficiency identified must be managed through mitigating actions. This requires receiving relevant indicators from entities on a regular basis. Specifically, quantitative information (RCSA[10] results, AML-CTF processes related metric indicators (SARs[11], backlogs, etc.)), Periodic and Permanent control results (Incidents, etc.), and qualitative information (Governance, any potential dysfunction, AML-CTF project updates, status of remedial action plans, Policy/Procedure updates, etc.).

3 ML-TF Risk Classification

The ML/TF risk classification exercise is the cornerstone of the Group's AML-CTF framework pursuant to which the Group and its entities define, adapt and improve their AML/CTF procedures and control framework in accordance with the inherent risks identified and assessed across their activities.

This exercise is performed at Group and at Entity level pursuant to the ML-TF risk Classification procedure (CPL0254/INS-CPL-FS66), combining a top-down and bottom-up approach for a comprehensive risk management framework.

3.1 Group ML-TF risk classification

The Group ML/TF Risk Classification Procedure defines a methodology under which Group Financial Security identifies, assesses, and documents ML/TF inherent risks with the appropriate level of granularity in relation to BNP Paribas activities Group-wide. Inherent risk is assessed in the following five axes prescribed by law applicable to the Group: geography, products & services, channels, transaction types and clients.

Identifying ML/TF risk areas under the Group-wide methodology results in:

- a common approach to assessing risk to be used by all Assessment Units[12] in their ML/TF Risk Classifications
- appropriate and relevant AML/CTF procedures and risk-based framework at Group level.

The Head of GFS Paris & KYC, responsible for the Group AML/CTF framework, validates the Group ML/TF Risk Classification and informs the Group Board of Directors of the outcome of the exercise.

The Group ML/TF Risk Classification must be updated at least annually and more frequently whenever there are material changes to the Group ML/TF risk profile.

As defined in the INS-CPL-FS66 ML/TF Risk Classification Procedure, BNP Paribas Cardif – as an insurance group – builds its own consolidated ML/TF Risk Classification on a yearly basis.

[10] Risk and Control Self-Assessment

[11] Suspicious Activity Reports

[12] Group Compliance has defined an Assessment Unit as a BNPP legal entity ("LE"), grouping of BNPP legal entities or part of a Legal Entity, identified and defined generally among usually a single Compliance Perimeter ("CP"), by activity type (transaction type, client type, service/product offerings, etc.) and geographic location for purposes of assessing risk. An AU can either comprise a single LE, or in some cases several LEs.

3.2 Entity ML-TF Risk Classification

Entities through Assessment Units complete a ML-TF risk classification for their activity based on the common methodology defined by the Group. Each Assessment Unit ML-TF risk classification is completed based on:

- risks identified in the Group ML-TF risk classification
- and ML-TF inherent risk with respect to the activity of the AU.

The ML/TF Risk Classification provides an in-depth view of the ML-TF inherent risks of each Assessment Unit, allowing AUs to deploy a risk-based AML/CTF framework to adequately cover risk.

Assessment Units ML/TF Risk Classifications must be updated at least once a year, or more frequently when there are material changes to their ML/TF risk profile.

4 AML-CTF Framework [13]

Every employee is involved in the fight against money laundering and terrorist financing

The Business, identified as the risk owner and 1rst line of defense, is the clients' entry point to the Bank/ BNP Paribas Cardif. The Business should:

- perform thorough diligences as per the KYC and other ("Know your Client" or other counterparties[14]) Policies
- maintain good knowledge of the business relationship
- identify and escalate any unusual behavior and/or activities to Compliance (cf section 4.3 for further details related to Unusual Activity Report "UAR").

Compliance, as the AML-CFT subject matter expert and 2nd line of defense, should:

- define a risk-based AML-CTF framework which is proportionate to and sufficiently mitigates the risks identified
- support the Business to implement and apply the Group standards.

The Group's AML-CTF framework must be deployed based on a corpus of procedures which defines the standards and principles to be applied throughout the Group.

In addition, the overall framework must be supported by a robust organization within the Group and its entities. Specifically:

- The AML-CTF framework is under the ultimate responsibility of the Head of AML-CTF framework (whether at Group or Entity level). The Head of AML—CTF framework holds a senior management position and possesses adequate knowledge, skills, competencies and experience to ensure the implementation of organizational and operational structure of the AML-CTF set-up described below.

[13] The Anti-Corruption framework and its related Policy (Global Anti-Corruption Policy – CPL0183/INS-CPL-FS06) are now part of Professional Ethics. As one of the predicate offences that concurs to launder money, corruption is also taken into consideration in the AML-CTF framework.

[14] Under this policy, the term "counterpart" refers to non-client business relationships (e.g. intermediaries, business partners, stakeholders, suppliers, banks…) which are subject to specific due diligence (e.g. KYI, KYS, KYB, KYX…).

- Supervision of ML-TF risks are also the responsibility of Senior Management, the Executive Committee and/or Board of Directors' concern. They play a key role and undertake great responsibility in managing the Group's overall risks. Assisted by the Head of AML-CTF framework, among others, they are the ultimate decision maker regarding major AML-CTF related topics based on information reported during the relevant committees on a regular basis (e.g. CCIRC[15] (Comité de Contrôle Interne des Risques et de la Conformité), GSCC (Group Supervisory and Control Committee)).

- Adequate and appropriate resources are properly managed and trained to perform the AML-CTF related duties. For certain tasks, the Group and/or its entities may utilize outsourcing or offshoring services that should be maintained in accordance with the related group procedures[16].

- Systems and tools support the overall set-up and facilitate compliance with regulatory requirements

- The framework is up-to-date and reviewed regularly in the context of newly identified/emerging risks, regulatory updates, etc.

- Data and/or information must be retained and kept in compliance with applicable laws and regulations taking into account related processes, jurisdictions[17], etc. Record keeping provisions are included into the related AML-CTF procedures where relevant.

4.1 Know your Client and Counterparties

The Group's Know Your Client (KYC) framework is the foundation of the AML-CTF framework and is an essential component of the overall set-up. The KYC framework has been broadened to specific counterparties[18] (e.g., suppliers (KYS), intermediaries (KYI), other counterparties (KYX), etc...).

From the onboarding to the termination of a business relationship, the Know Your Clients and/or Counterparties standards must be applied throughout the life of the business relationship and in accordance with the Global KYC policies (CPL0252/INS-CPL-FS25 and all related segment policies) and other policies (KYS, KYI, KYX, etc.).

[15] Internal Risks and Compliance Control Committee

[16] Please refer to procedures DG0052 and RISK0417 and any procedure allowing outsourcing/offshoring of AML-CTF tasks.

[17] E.g., As per the French Monetary and Financial code, any information collected in the course of our AML-CTF vigilance obligations must be retained 5 years after closing the client's account or after the end of the relationship and any information on transactions during 5years after its execution. Timeframes can be different according to each part of AML-CTF framework.

[18] Within this policy, the term "counterpart" is used to cover all the Group's business relationships (e.g. business partners, stakeholders, suppliers, banks…) different from the client

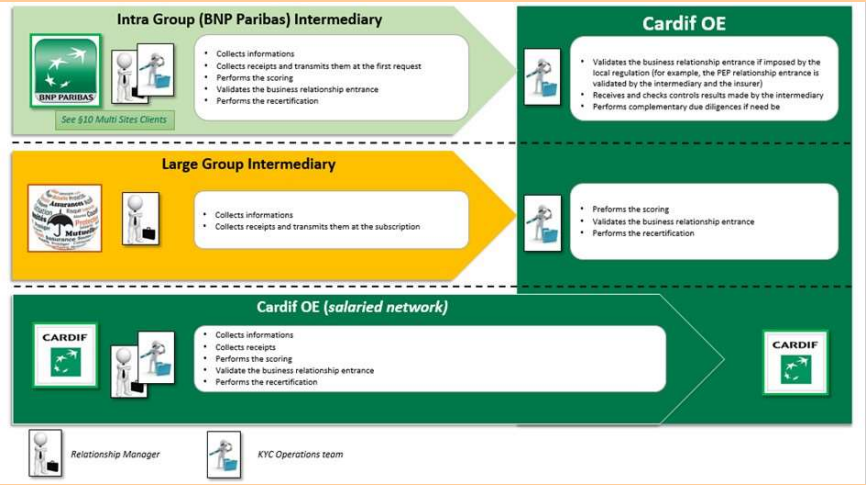
Below are the essential components of KY Clients and/or Counterparties (e.g. intermediaries, suppliers, banks…):

- **When does** KY Clients and/or Counterparties occur? KY Clients and/or Counterparties begin before entering into relationship with each client/counterpart supplier, etc. relationship; over the life of that relationship, when specific trigger events occur and before terminating such relationship.
- **What does** KY Clients and/or Counterparties **involve?** Information/documents are collected from the client or from any other sources to identify the client/counterpart, its Ultimate Beneficial Owners (UBOs) and related persons and in order to understand the nature and purpose of the business relationship. This information enables an entity to identify risk factors related to its clients/counterparts, supplier etc. (e.g., geography, sector, etc.) which are used to determine the score, take a decision on the acceptance, maintenance or refusal of the business relationship.
  In some cases, additional measures must be deployed especially when entering in and/or maintaining a high -risk relationship19 (e.g., business relationships with Politically Exposed Persons (PEP), Correspondent Banking (CBK), client domiciled/incorporated or established in high-risk third country).
- **Who performs** KY Clients and/or Counterparties**?** KY Clients and/or Counterparties tasks are assigned to relevant stakeholders to promote a robust process and mitigate conflicts of interest, error and fraud. The relationship manager[20] plays a primary role in this process and must exercise constant vigilance over the business relationship. KY Clients and/or Counterparties Operations, the Business Unit's Management and Compliance also play key roles in the course of the KY Clients and/or Counterparties process.

Cardif relies on "tierce introduction" (introduction by a third party) as defined in the Monetary and Financial Code in Article L 561-7 to authorized intermediaries. In these case, Clients are not assigned to a Cardif Relationship Manager.

<u>The diagram below shows the roles and responsibilities of the Relationship Manager and the KYC Operations team according to the distribution model:</u>

<u>What does OE stand for?</u>



- **Why is** KY Clients and/or Counterparties **essential?** Reliable and up to date KY Clients and/or Counterparties data is critical to identify higher risk clients and/or counterparties and implement the appropriate levels of due diligence required. It also allows the Bank in the course of transaction monitoring

[19] Cf Global KYC Policy (CPL0252/INS-CPL-FS25)

[20] or equivalent function where such position does not exist

to assess whether clients are using their accounts or the Bank's products and services in ways that appear unusual or inconsistent with the expected use of the account.

Please refer to INS-CPL-FS25 Know Your Client - Global Policy and also refer to applicable Group's KYC segment policies available on Echonet (Procedure Group) for further instructions.

4.2 Payment Transparency

Not Applicable to BNP Paribas Cardif: Following FATF Recommendation 16 and EU Regulation 2015/847, transactions, whether they are cross border or domestic transfers, must be performed and executed in full transparency. This requires banks and financial institutions to provide accurate and meaningful information about the originator and beneficiary of any wire transfers.

The Group has implemented measures to ensure compliance with payment messaging principles. The Group's strong commitment is reflected in its framework that relies on applying the most stringent rules as the Group Payment Transparency procedure (CPL0154). This procedure requires complete information for all incoming and outgoing payments regardless of where the Payment Service Provider is located. In its effort to enhance its set up, all flows are controlled and any payments with missing information can be rejected or suspended.

Furthermore, the Group imposes restrictive measures to regularly failing banks such as increasing their risk level for higher scrutiny or terminating the relationships and reporting such institutions to the French authorities.

Missing or incomplete information raises doubt about the economic legitimacy of a transaction; if doubt persists, such alert is a suspicious transaction indicator for possible Suspicious Activity Reports ("SAR") reporting.

4.3 Transaction Monitoring

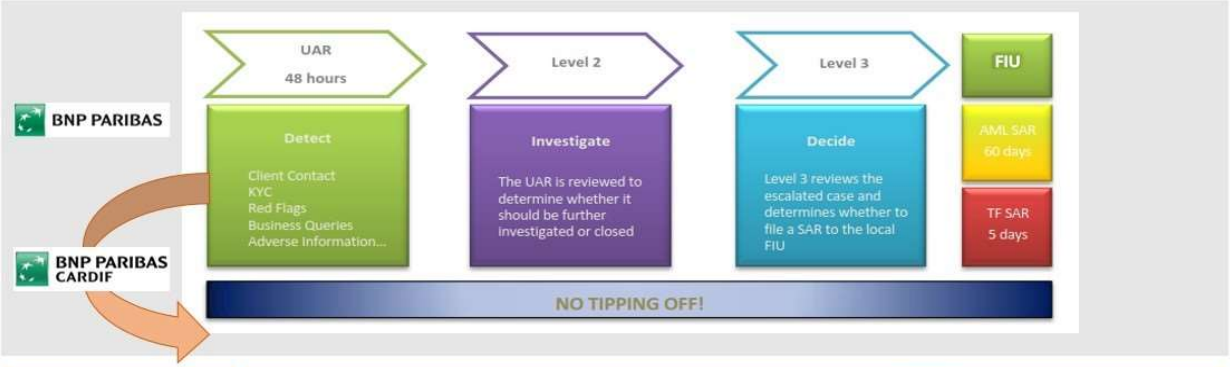
To satisfy regulatory obligations to detect and report any suspected cases of money laundering, corruption and terrorist financing to the national Financial Intelligence Units ("FIUs"), the Bank/ BNP Paribas Cardif constantly monitors its transactions. The Group relies upon the sound knowledge of its business relationships, reliable data, accurate, up-to-date and complete KYC to implement a risk-based and robust monitoring framework based on both constant vigilance and manual and/or automated transactions monitoring.

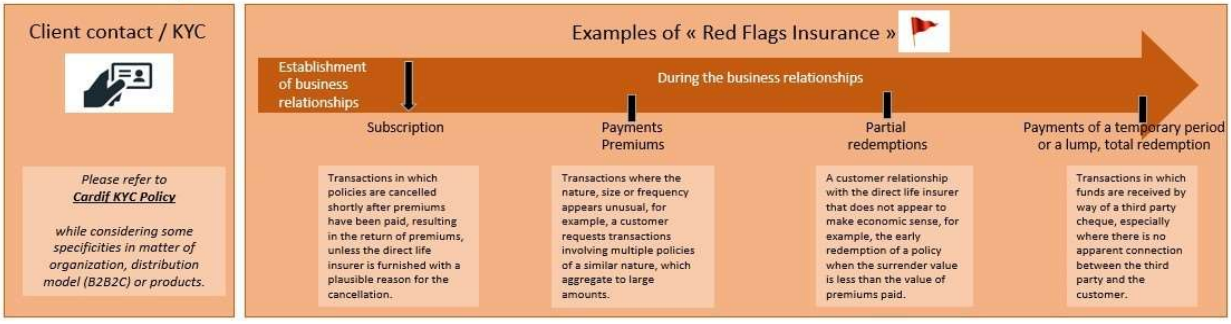
Detecting suspicious activities and unusual behavior requires every employee's constant vigilance while interacting with clients. Building a good knowledge of a client's transactional profile and identifying potential anomalies are critical components in the timely identification of unusual activity. The transaction monitoring framework is comprised of several components:

- Detection solutions, based on various AML-CTF red flags that identify unusual and suspicious transactions. The Group Detection Solution catalogue outlines the minimum standards to detect risky and unusual behaviors. Entities must deploy consequently an adequate AML-CTF Transaction Monitoring ("AML-CTF TM") framework covering, at a minimum, the Group Detection Solutions that are applicable to them.

- Analysis and investigation of all cases escalated by employees (Unusual Activity Reports("UAR")), generated by manual and/or automated tools, as well as those that arise from public authorities, peers or press (i.e., external triggers)

BNP Paribas Cardif has created a "Practical Guide" –in the INS-CPL-FS55 – to ensure all employees apply a homogeneous methodology for detecting unusual activity, and consider the following specificities:





- Filing of Suspicious Activity Reports ("SAR") with the national FIU when a doubt remains after the case has been fully investigated and/or whenever local regulation requires.

- Post-SAR actions, including termination of business relationships when necessary. The general principle set out by the Group is to terminate the business relationship with the client and related person following a SAR filing, as it is considered that any suspicion hampers the Bank's confidence in the business relationship. Exceptions to this general principle may be considered (e.g., client is a victim, SAR filed on a counterparty of the client, etc).

The AML-CTF TM framework is implemented through shared responsibility and close coordination between

- The Business, acting as the first line of Defense and responsible for detecting unusual and/or suspicious transactions and behaviors; and
- Compliance who, acting as the second line of Defense, performs further investigations and files SAR where necessary.

All these principles are provided in the following policies:

- The AML-CTF Transaction Monitoring Procedure (CPL0287/INS-CPL-FS55) applicable to Savings activities outlines these principles,
- The Global Anti-money Laundering & Counter Terrorist Financing Policy for Insurance protection business (INS-CPL-FS56) applicable to protection activities also outlines these principles.

4.4 Counter Terrorist Financing

Countering the financing of acts of terrorism, terrorists and terrorist organizations is an integral part of the financial security obligations of the BNP Paribas Group.

Fighting terrorist financing effectively involves implementing adequate measures throughout the Group to prevent the occurrence of such events.

The Group Counter Terrorist Financing framework sets forth measures to identify persons involved in networks that directly or indirectly support any persons or organizations involved in preparing or committing an act of terrorism. Such measures also include the detection of logistical operations to the preparation of an act of terrorism, the identification of suspicions immediately after an act of terrorism, and the potential tracking of suspects in cooperation with relevant authorities.

Counter-Terrorist Financing follows a prevention, detection, and reporting logic that is similar to that of Anti Money-Laundering, but the main difference lies in how detection measures are deployed, i.e:

- The detection modalities rely mostly on cumulative weak signals, external triggers and applicable Sanctions lists; and
- The Reporting timeframe must be as short as possible in order to efficiently prevent the occurrence of an act of terrorism.

For further details regarding Counter Terrorism Financing, please refer to Global CTF Policy – INS-CPL-FS68.

4.5 Country Policy

With a presence around the world, BNP Paribas offers worldwide financial services to its clients. In line with the Group's strategy, BNP Paribas' ambition is to continue to serve its clients while enhancing the security of the transactions they entrust to the Group and the security of the Bank.

In that respect, the Group has taken a proactive approach through a dedicated internal policy, the Policy applicable to countries where the Group has no physical presence (CPL0248/ INS-CPL-FS19) commonly called as the "Country Policy" which aims at being very selective in the way the Bank operates in non-EU and non-OECD countries and where it has no physical presence.

Besides the Major Sanctioned Countries (and Regions) ("MSCs"), the countries where the Group is not present are classified, based among others on the countries Financial Security sensitivity risk[21], into 4 categories: P0, P1, P2 and P3 countries, ranked by decreasing order of risks. The Country Policy defines the conditions under which business can be conducted in these countries.

For further information:

- INS-CPL-FS19 Country policy
- INS-CPL-FS35 Global Sanctions Policy
- INS-CPL-FS39 Cuba Policy
- INS-CPL-FS40 Group procedure concerning the situation in Ukraine and Crimea Sevastopol - Related sanctions
- INS-CPL-FS41 - Relationships Involving Individual Nationals and Residents of the Major Sanctioned Countries (and Regions) of Iran, Syria, North Korea and Crimea/Sevastopol

[21] Countries' Financial Security sensitivity is a risk level assessed using an internal methodology that combines a combo of criteria such as poor governance (unstable institutions, poor regulatory framework) instability (armed conflict), the level of corruption, money laundering and organized crimes, privileged tax regimes, etc. As a result of this assessment, countries are rated as Low, Medium, High or Very High Sensitive impacting the score of a client incorporated or having business in sensitive countries. List of sensitive countries can be found in the GFS SharePoint

4.6 Sensitive Banks Management

As one of the major actors of the financial sector, the Group is continuously in relationship with other banks, acting either as "clients/counterparties" or as "vectors" of operations for individuals and non-individuals. The Group has therefore set principles and standards to manage on a risk-based approach its relationships with banks presenting a particular high level of risk (called "Sensitive Banks"). Relationships with such banks are restricted or terminated for compliance reasons as per the Sensitive Bank Management Framework Procedure (CPL0195/ INS-CPL-FS53).

4.7 Information Sharing

Information sharing is a critical pillar of an effective AML-CTF framework. As such, the Group has defined a framework to ensure that AML/CTF information related to clients and transactions is shared in accordance with applicable International[22], European[23] and local requirements.

Sharing AML/CTF information between two or more BNP Paribas entities significantly increases the efficiency and effectiveness of the Bank's AML/CTF framework. This intra-Group AML-CTF information sharing involves finding a balance between the need to protect personal data that can circulate across the Group and the objective to fight against money laundering and terrorism financing.

In contrast sharing AML/CTF information outside the Group with other Financial Institutions is prohibited. Exceptions may be considered in very specific cases.

Whether information is shared internally or externally, it must be done by each Entity in compliance with the Group standards and subject to their applicable local laws.

Finally, BNP Paribas Group is required to supervise the efficiency of its information sharing framework. Thus, the Group must identify entities that raise obstacles to information sharing due to their local laws and regulation. To do so, the relevant entities must notify GFS Paris & KYC of such obstacles, so that possible measures can be put in place to mitigate them.

4.8 Training

The complexity of the AML-CTF regulatory environment requires skilled and trained resources to implement the AML-CTF framework, thereby protecting the Bank from reputational damage and civil, criminal and/or administrative penalties (including monetary penalties).

The Group, in compliance with Group Policy on AML-CTF training (CPL0295)/ INS-CPL-FS45, has deployed a centralized AML/CTF training program for all BNP Paribas employees and external staff such as temporary employees. The objective is to ensure that the target population is assigned to and completes training commensurate with the nature of their tasks and their exposure to ML/TF related risks.

For further information: see INS-CPL-FS45 Group policy on Anti Money Laundering and Counter Terrorist Financing trainings.

[22] Such as FATF guidelines, Recommendation 18

[23] Such as General Data Protection Regulation, Article 45 of EU Directive 2015/849

4.9 Permanent and Periodic Controls

Applying relevant controls is a sine qua non condition within BNPP's AML-CTF framework to ensure its effectiveness. Internal controls measure the effectiveness of the AML-CTF set up and allow management to identify areas of improvements and prioritize corrective measures to be deployed.

With its control framework organized[24] around Three Lines of Defense, every BNP Paribas employee is involved in the management of its risks.

The First and Second Lines of Defense are deploying a permanent control set up, as described respectively in the Compliance LoD1 Generic Control Library (CPL0328/ INS-GCP-LOD1-FS) and the Compliance Control Plan (SF0029/ INS-GCP-CPL1-FS).To complement these control plans, a risk assessment exercise (Risk Control Self-Assessment (RCSA)), owned by the Business, is also performed on a yearly basis by each Entity. The RCSA provides a comprehensive view of entities' inherent risk, control environment, and residual risk. As a result, mitigating actions are identified and deployed to improve the AML-CTF control environment.

In addition, the permanent control framework is complemented with the periodic control performed by the Inspection Générale (IG) acting as the Third Line of Defense.

Both results of permanent and periodic controls are reported to the Management Body, notably through the Internal Control Committees.

4.10 Management Information and Reporting

In addition to the pillars detailed above, an effective AML/CTF framework is contingent on the definition, deployment and reporting of relevant metrics regarding the:

- AML/CTF framework implementation and maintenance (major developments, policies, risk classification updates, etc.)
- AML/CTF framework effectiveness (KYC indicators, AML-CTF TM indicators, internal control results, etc.)

These metrics must be reported on a regular basis to the appropriate stakeholders (management, etc.). They aim at highlighting risk areas and any potential deficiencies in the framework, so that appropriate mitigating actions can be deployed.

Furthermore, each entity is responsible to fulfill their regulatory reporting obligations and submit within their legal timeframe the regulatory reports[25] that are required by their local regulations.

[24] French regulated entities must appoint a Head for the AML-CTF Permanent Control (e.g. Head of Compliance) and a Head for the AML-CTF Periodic Control (e.g. Head of IG) as part of the AML-CTF framework and its implementation.

[25] Regulatory reports in France include notably the Etats Blanchiments (AML/CTF related questionnaire) for banking and insurance activities to be submitted to the ACPR, Internal Control Reports (called "RACI" (Rapport Annuel de Contrôle Interne) to be submitted to the ACPR for banking and insurance activities and AMF for asset management activities.

5 GLOSSARY

ACPR	Autorité de Contrôle Prudentiel et de Résolution	French Prudential and Resolution Supervisory Authority
AML	Anti-Money Laundering	Fight against laundering the illegal proceeds of predicate offences (see definition herein).
AML/CTF-TM	Anti-money laundering / Counter Terrorist Financing Transaction Monitoring	Process by which alerts are identified and handled to determine whether they should be reported as suspicious transactions to the local FIU within the reporting timeline.
CTF	Counter Terrorist Financing	Fight against terrorist financing.
FATF	Financial Action Task Force	Intergovernmental body composed of member states that adhere to the recommendations, global standards and monitoring for combating money laundering and terrorist financing.
FIU	Financial Intelligence Unit	Local authority to which SARs are reported (e.g., France: TRACFIN).
GFS	Group Financial Security	Compliance domains dedicated to Financial Security risks (GFS Paris & KYC and GFS US which is dedicated to OFAC compliance).
IG	Inspection Générale	General Inspection, the Group's 3rd line of defense which exercises periodic controls.
KYC	Know Your Client	Due diligence standards for client knowledge.
PSP	Payment Service Provider	Providers that accept electronic payments by a variety of payment methods using credit cards, bank-based payments such as direct debit, bank transfer, real-time transfers –on-line banking).
R16	Also known as FATF R16	Regulation on information Accompanying Transfers of Funds (EU Regulation 2015/847), to provide identifying information on the originator and beneficiary for wire transfers. Entered into force concurrently with the 4th Money Laundering Directive on June 26, 2017.
SAR	Suspicious Activity Report	A formal filing to the local FIU indicating possible money laundering or terrorist financing. It is a regulatory obligation of financial institutions under local law.
UAR	Unusual Activity Report	A manual alert escalated by the front line or any other employee to Compliance for further investigation and potential filing of a SAR if suspicion remains

ORGANIZATION OF AML-CTF PROCEDURES