

DOCUMENTO ANALITICO IN MATERIA DI ANTIRICICLAGGIO E CONTRASTO AL FINANZIAMENTO DEL TERRORISMO

BNP Paribas Cardif Vita S.p.A.

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

Versione 1.0 [21/12/2023]



**BNP PARIBAS
CARDIF**

The insurer
for a changing
world

QUADRO GENERALE DEL DOCUMENTO

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

Livello	Livello 3
Tipologia documento*	2- Organization documents
Ambito di applicazione*	Cardif Vita (132 007)
Da adattare localmente*	Specifica
Classificazione*	Pubblica
Accesso	Tutto il personale
Autore	Viviana Becchi
Unità organizzativa dell'autore*	Compliance
Organo responsabile per l'approvazione*	Amministratore Delegato
Contributors*	Customer Service - Operations Controls, Risk Management, Internal Audit, Legal & Corporate Affairs

Codice*	IT-CPL-51-IT
Versione*	1.0
Data di Validazione*	21/12/2023
Data di efficacia*	21/12/2023
Frequenza di revisione	Annuale

Norme correlate	- D. Lgs. n. 231/2001 - D. Lgs. n. 109/2007 - D. Lgs. n. 231/2007 - Regolamento IVASS n. 44/2019 - Regolamento IVASS n. 111/2021
Documenti correlati	- Modello di Organizzazione, Gestione e Controllo ex D. Lgs. n. 231/01 - IT-GOV-05-IT Conduct Policy - IT-CPL-35-IT Politica di Conformità - CAN 03-03-22 Processo Decisionale Compliance - IT-CPL-10-IT Politica Antiriciclaggio - INS-CPL-FS01 Cardif's Global Anti-Money Laundering & Counter Terrorist Financing Policy - CAN 03-02-02 KYC & Due Diligence per la Clientela Diretta Interna - IT-CPL-23-IT Politica applicabile alle relazioni con Persone Politicamente Esposte (PEP) - INS-CPL-FS60-HO Procedure on the decision to enter into business relationships with politically exposed persons and correspondent banks - CAN 03-03-13 Comportamento fraudolento dei dipendenti - IT-CPL-24-IT Know Your Client - Global Policy (KYC) - CPL0253-HO KYC - Corporates & Small Businesses - CPL0260-HO KYC - Private Investment Vehicles - CPL0266-HO KYC - Retail Markets & Private Banking - CPL0269-HO KYC - Non profit Private Entities - IT-CPL-20-IT Know Your Intermediary - IT-CPL-34-IT Framework generale inerente il processo di validazione delle attività nuove - modificate e delle transazioni eccezionali - IT-CPL-46-IT Operazioni Sospette di riciclaggio e/o connesse al terrorismo - IT-CPL-13-IT Monitoraggio delle Transazioni e Gestione degli Alert (AML-TM) - IT-CPL-21-IT Policy Anticorruzione - IT-CPL-28-IT Dispositivo di Allerta Etico - INS-CPL-REG03-HO FATCA General Procedure - INS-CPL-REG04-HO AEOI General Procedure



	- IT-CPL-44-IT Antiriciclaggio - Tenuta AUI: Rapporti Continuativi e Operazioni Monetarie - INS-CPL-FS36-HO Screening of Relationships - IT-CPL-05-IT Procedura per la gestione delle liste di sicurezza finanziaria - IT-MKT-01-IT Sviluppo e Validazione Prodotti Saving - IT-MKT-02-IT Sviluppo e Validazione Prodotti Protection - IT-CPL-26-IT Erogazione formazione Compliance e Sicurezza Finanziaria al personale - IT-OPS-16-IT Gestione Portafoglio CPI e Protezione - IT-OPS-17-IT Gestione Post Vendita Loans & Protection - IT-OPS-10-IT Post Vendita Saving - IT-OPS-11-IT Post Vendita Non Finanziario Saving - IT-OPS-12-IT Liquidazione Riscatti e Scadenze Saving - IT-OPS-13-IT Liquidazione Sinistri Saving - IT-OPS-08-IT Assunzione Prodotti CPI - IT-OPS-14-IT Emissione contratti Saving - IT-OPS-30-IT Gestione Sinistri Loans & Protection - LDI 09-01-02 Gestione sequestri e comunicazioni al FUG - LDI 09-01-03 Gestione in full outsourcing del portafoglio risparmio in run off - IT-OPS-01-IT Gestione Polizze Dormienti - IT-PROC-02-IT Controllo attività in outsourcing - IT-CPL-30-IT - Comitato Accettazione Clienti (CAC) - IT-CPL-01-IT Analisi della clientela - Secondo Livello - CAN 01-04-02 Attività da eseguire per l'invio delle segnalazioni in caso di operazioni sospette - IT-OPS-26-IT Gestione Alert Operazioni Sospette Analisi e controlli di primo livello - IT-OPS-33-IT Due Diligence Clientela Esterna-Interna - IT-OPS-34-IT Gestione degli eventi sospensivi - IT-REGC-04-IT Liste e sblocchi pagamenti - IT-OPS-25-IT Gestione AUI: Archivio Unico Informatico Cardif - Nota operativa: Residenti all'estero - Nota operativa: Acquisizione da Servizio Italia dell'attestazione relativa all'assolvimento dell'adeguata verifica
--	--

Parole chiave	Antiriciclaggio, Antiterrorismo, Adeguata verifica, Sanzioni finanziarie internazionali
Sintesi	Il Documento Analitico è il documento con cui l'Alta Direzione, ai sensi del Regolamento IVASS 44 / 2019, definisce le scelte concrete effettuate sui diversi profili rilevanti in materia di: i. assetti organizzativi, procedure e controlli interni, ii. conservazione dei dati, iii. adeguata verifica, incluse le specifiche misure semplificate e rafforzate.

**campi obbligatori*

STORICO VERSIONE/ MODIFICHE APPORTATE

N. versione	Data entrata in vigore	Descrizione della modifica	Autore della modifica
V1	21/12/2023	Prima versione	V. Becchi



EXECUTIVE SUMMARY

Il presente documento relativo a Cardif Vita S.p.A. è redatto in linea con le previsioni del Regolamento IVASS n. 44/2019 definisce in dettaglio (i) gli assetti organizzativi, le procedure implementate e i presidi di controllo interni, (ii) le modalità di conservazione dei dati adottate, nonché (iii) i processi in materia di adeguata verifica della clientela in considerazione di un approccio basato sul rischio.

I. OGGETTO E AMBITO DI APPLICAZIONE	8
II. NORMATIVA DI RIFERIMENTO	9
III. MODELLO DI GOVERNO DEL RISCHIO DI RICICLAGGIO E FINANZIAMENTO DEL TERRORISMO	10
3.1. Principi generali	10
3.2. Assetto organizzativo	10
3.2.1. Organi sociali	11
3.2.1.1. Consiglio di Amministrazione	11
3.2.1.2. Amministratore Delegato	11
3.2.1.3. Collegio Sindacale	11
3.2.1.4. Organismo di Vigilanza ex D. Lgs. n. 231/01	11
3.2.1.5. Comitato per il Controllo Interno e i Rischi (CCIR)	12
3.2.2. Strutture e Uffici posti a presidio del rischio di riciclaggio e di finanziamento del terrorismo	12
3.2.2.1. Funzione Compliance e Funzione Antiriciclaggio	12
3.2.2.2. Responsabile della Funzione Antiriciclaggio e Responsabile / Delegato per le segnalazioni delle operazioni sospette (SOS)	17
3.2.2.3. Regulatory Controls	18
3.2.2.4. Internal Audit	19
3.2.2.5. Risk Management	19
3.2.2.6. Altre unità organizzative aziendali	20
3.2.3. Comitati a presidio del rischio di riciclaggio e di finanziamento del terrorismo	21
3.2.3.1. Comitato Antiriciclaggio	21
3.2.3.2. Comitato di Sicurezza Finanziaria	22
3.2.3.3. Comitato Accettazione Clienti e KYC Review	22
3.2.3.4. Comitato Accettazione Intermediari (IAC)	23
3.3. Flussi informativi e reporting	24
3.3.1. Relazioni tra la Funzione Antiriciclaggio ed il Gruppo	28
3.3.2. Rete distributiva diretta	29
IV. STRUMENTI A SUPPORTO DELL'OPERATIVITÀ	30
4.1. Applicativi gestionali e tool post-vendita	30
4.2. Applicativi di screening, scoring e conservazione dei dati AML	31
V. MAPPATURA DEI RISCHI	33
5.1. Individuazione del rischio	33
5.2. Alimentazione del Risk Register	33
VI. ANALISI E VALUTAZIONE DEL RISCHIO DI RICICLAGGIO E FINANZIAMENTO DEL TERRORISMO	34
6.1. Autovalutazione IVASS	34
6.1.1. Impostazione dell'analisi	35
6.1.2. Analisi e valutazione dei rischi e dei controlli	35

6.1.3.	Predisposizione della relazione di autovalutazione e del remedation plan	37
6.1.4.	Compilazione del prospetto IVASS	38
6.2.	Group Risk Assessment exercises.....	38
VII.	DUE DILIGENCE DELLA RETE DISTRIBUTIVA	39
VIII.	ADEGUATA VERIFICA E VALUTAZIONE DEL RISCHIO DELLA CLIENTELA	41
8.1	Acquisizione delle informazioni per i prodotti Savings	42
8.2	Acquisizione delle informazioni per i prodotti Protection	44
8.3	Verifica delle informazioni	45
8.4	Determinazione del profilo di rischio della clientela.....	46
8.4.1	Profilo di rischio acquisito da BNL.....	48
8.1.1	Profilo di rischio acquisito da Cardif Lux	48
8.2	Misure semplificate di adeguata verifica	49
8.3	Misure rafforzate di adeguata verifica	50
8.3.1	Assegnazione status PEP	52
8.3.2	Blocchi sospensivi.....	52
8.3.3	Acquisizione da parte delle Società Fiduciarie dell'attestazione di adeguata verifica	53
8.4	Ricertificazione del cliente	54
8.4.1	Ricertificazione periodica	54
8.4.2	Ricertificazione ad evento.....	54
IX.	PROCESSI DECISIONALI E COMITATI	55
9.1.	Comitati CAC e KYC Review	55
9.2.	Comitato Antiriciclaggio	55
9.3.	Comitato Sicurezza Finanziaria	56
X.	TRANSACTION MONITORING	56
XI.	Gestione delle operazioni sospette	58
XII.	Controlli di primo e secondo livello	60
XIII.	OBBLIGHI DI CONSERVAZIONE	61
11.1	Conservazione dei documenti	61
11.2	Conservazione dei dati e delle informazioni	62
XIV.	FORMAZIONE	63
XV.	Appendix: Acronimi/Definizioni	65



I. OGGETTO E AMBITO DI APPLICAZIONE

Il presente documento (di seguito anche “documento analitico” o “il documento”) è redatto ai sensi dell’articolo 11, comma 1, lettera c) del Regolamento IVASS n. 44 del 12 febbraio 2019 (di seguito anche “il Regolamento”) come modificato dal Provvedimento IVASS n. 111/2021.

In particolare con il presente documento, in coerenza con i criteri generali in materia di antiriciclaggio e contrasto al finanziamento del terrorismo individuati dal Consiglio di Amministrazione di Cardif Vita S.p.A. (di seguito anche “Cardif Vita” o “Compagnia”) nella “Politica Antiriciclaggio” per la gestione del rischio di riciclaggio e finanziamento del terrorismo, l’Alta Direzione¹ di concerto con la Funzione Antiriciclaggio definisce le scelte operative che dovranno essere osservate con riferimento i seguenti profili:

- la predisposizione e il mantenimento di idonei **assetti organizzativi, procedure e controlli interni**;
- la **conservazione dei dati**;
- lo svolgimento della **adeguata verifica** della clientela, incluse le specifiche misure semplificate e rafforzate.

L’Alta Direzione, anche a seguito di preventivo consulto e di analisi delle risultanze delle attività di controllo e di *risk assessment* effettuate da parte della Funzione Antiriciclaggio, assicura nel tempo, la coerenza del documento analitico con l’effettiva esposizione al rischio di riciclaggio anche al fine di dimostrarlo alle Autorità, come previsto dall’articolo 11 comma 1 lettera d) del Regolamento.

Il presente documento è soggetto alla verifica dei contenuti da parte della Funzione Antiriciclaggio, quindi, sottoposto all’approvazione dell’Alta Direzione, nonché sottoposto a revisione ogniqualvolta vi siano delle modifiche alle scelte concrete effettuate dalla Compagnia in materia di assetti organizzativi, procedure e controlli interni, adeguata verifica della clientela, conservazioni di dati e documenti.

In conformità con quanto previsto dall’articolo 14, comma 2, lettera k), del Regolamento IVASS, oltre alla effettuazione di attività di supporto all’Alta Direzione, la Funzione Antiriciclaggio concorre a predisporre ogni utile integrazione e/o aggiornamento del documento, nonché, a seguito dell’ approvazione, procede a renderlo disponibile a tutto il personale² e alla rete distributiva diretta, promuovendo in tal modo la diffusione della cultura del controllo finalizzata alla sensibilizzazione degli stessi soggetti sull’importanza ed utilità dei controlli interni.

Il documento analitico rientra all’interno di un quadro organico di disposizioni interne in materia di antiriciclaggio e contrasto al finanziamento del terrorismo, che ricomprende anche:

- la **normativa del Gruppo BNP Paribas** (di seguito “Gruppo”) che identifica le linee strategiche e le indicazioni in materia di gestione del rischio di riciclaggio e di finanziamento al terrorismo che per la Compagnia vengono, in primo luogo, stabilite attraverso la “Global Anti-Money Laundering & Counter Terrorist Financing Policy”³ di BNP Paribas Cardif, nell’ambito dell’attività di direzione e coordinamento da questa esercitata, quindi, implementata localmente mediante ogni necessario e/o opportuno adeguamento;
- **policy aziendali**. All’interno di tale categoria rientrano:
 - le “linee guida” a contrasto e/o mitigazione dei rischi, così come fornite dal Gruppo volte alla definizione dei principali obiettivi in un determinato ambito di attività, recepite dalla Compagnia. Tale recepimento da parte della Compagnia avviene considerando il proprio modello di business e l’operatività posta in essere dalla stessa, nonché eventuali specificità della normativa locale;
 - indirizzi e orientamenti individuati dal Consiglio di Amministrazione che disciplinano gli aspetti di carattere strategico, i valori fondamentali, i criteri ed i principi sui quali si fondano le scelte organizzative e gestionali della Compagnia. In tale categoria, è ricompresa la “Politica Antiriciclaggio” per la gestione del rischio di riciclaggio e finanziamento del terrorismo redatta ai sensi dell’articolo 10, comma 1, lettera b) del Regolamento IVASS, che illustra le scelte rilevanti in materia di assetti organizzativi, procedure e controlli interni, valutazione e gestione del rischio di riciclaggio e finanziamento del terrorismo, adeguata verifica della clientela, segnalazione di operazioni sospette, conservazione di dati e formazione;

¹ Qualora fosse confermato il testo del Documento di consultazione IVASS 4 / 2023 il presente Documento Analitico dovrà essere definito nel suo contenuto dall’Organo con funzioni di gestione.

² Il Documento è messo a disposizione del personale interno alla Compagnia sull’Intranet aziendale Echonet.

³ INS-CPL-FS01-V 11.

- **procedure**, documenti che formalizzano e normano l'insieme di attività che compongono un processo aziendale interno e trasversale, indicandone i tempi, le responsabilità, gli attori e i punti di controllo.

Il documento è integrato dai seguenti allegati⁴:

- Allegato 1 - Modello di profilatura Cardiff Vita;
- Allegato 2 - Eventi sospensivi;
- Allegato 3 - Regole_Operazioni Sospette_KYC4.

II. NORMATIVA DI RIFERIMENTO

Il presente documento è redatto in conformità con le disposizioni normative/regolamentari in materia di antiriciclaggio e contrasto al finanziamento del terrorismo di cui si elencano di seguito le principali⁵:

- D. Lgs. n. 231 del 21 novembre 2007 (di seguito "Decreto antiriciclaggio") modificato dal D. Lgs. n. 90 del 25 maggio 2017 e dal D. Lgs. n. 125 del 4 ottobre 2019 quest'ultimo contenente disposizioni attuative della Direttiva (UE) 2018/843 (V Direttiva AML) relativo alla prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo; nonché integrato dal D.lgs. 195/2021 contenente disposizioni attuative della Direttiva (UE) 1673/2018 (VI Direttiva AML).
- D. Lgs. n. 109 del 22 giugno 2007 modificato dal D. Lgs. n. 90 del 25 maggio 2017, recante misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale.
- Regolamento IVASS n. 44 del 12 febbraio 2019 e ss. m. e i., recante disposizioni attuative del Decreto antiriciclaggio in materia di organizzazione, procedure e controlli interni e di adeguata verifica della clientela, al fine di prevenire l'utilizzo delle imprese di assicurazione e degli intermediari assicurativi ai fini del riciclaggio e del finanziamento del terrorismo.
- Provvedimento IVASS n. 111 del 13 luglio 2021, in attuazione degli articoli 15 e 16 del D.lgs. 231/2007, che a modifica ed integrazione del precitato Regolamento n. 44/2019, reca le disposizioni in merito ai criteri e alle metodologie da utilizzare per individuare e valutare il proprio rischio di riciclaggio e stabilisce criteri dimensionali e organizzativi in base ai quali i soggetti obbligati istituiscono la Funzione Antiriciclaggio e Internal Audit, nominano i responsabili di tali funzioni e il Delegato per la segnalazione delle operazioni sospette.
- Ogni altro orientamento regolamentare in materia diffuso dalle Autorità locali.

Inoltre, dovranno sempre tenersi in considerazione gli standard internazionali e le fonti normative europee. Si ricordano in particolare le "Linee Guida sulla cooperazione e sullo scambio di informazioni tra le Autorità di vigilanza in materia di antiriciclaggio" emanate da EBA-ESMA ed EIOPA e le 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" (Trattato di Funzionamento dell'Unione Europea) sia anche per quanto richiamati dalla regolamentazione secondaria e attuativa degli adempimenti di Legge.

Quanto precede, dovrà in ogni caso tenere conto dei requisiti definiti a livello di Gruppo; qualora questi ultimi non siano perfettamente coincidenti con i requisiti locali dovranno privilegiarsi le regole più stringenti e/o rigorose e/o richiedenti un livello di dettaglio superiore in termini di dati, informazioni, documenti e/o controlli, salvo che l'applicazione non si ponga in contrasto con norme inderogabili di legge e/o provvedimenti dell'Autorità di Vigilanza.

Le norme sopra indicate intendono rafforzare, in linea con quanto previsto dalla normativa e dagli orientamenti europei in materia, i presidi antiriciclaggio, dando maggior spazio all'**approccio basato sul rischio** chiedendo alle **imprese e agli intermediari assicurativi** di farsi **parte attiva** nell'**individuazione** e nella **valutazione dei rischi** di riciclaggio e finanziamento del terrorismo ai quali sono in concreto esposti e nella scelta delle misure più adeguate a fronteggiarli.

⁴ Gli allegati al Documento sono resi disponibili all'interno della Intranet aziendale Echonet.

⁵ Si rinvia alla "Politica Antiriciclaggio" per un maggiore approfondimento della normativa esterna di riferimento in materia di antiriciclaggio e contrasto al finanziamento del terrorismo.

III. MODELLO DI GOVERNO DEL RISCHIO DI RICICLAGGIO E FINANZIAMENTO DEL TERRORISMO

3.1. Principi generali

La Compagnia si è dotata e mantiene un sistema di governo societario e dei rischi (AML) 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 e 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.

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

- istituzione e mantenimento di una Funzione Antiriciclaggio con nomina di un Responsabile della Funzione Antiriciclaggio e attribuzione di appositi compiti. La Funzione Antiriciclaggio è integrata all'interno della Funzione Compliance;
- 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 Delegato SOS;
- 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 esposizione complessiva ai rischi di riciclaggio e di finanziamento del terrorismo che emerge conducendo annualmente l'esercizio di autovalutazione;
- impegno ad agire 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;
- definizione di sistemi valutativi e processi operativi chiari, oggettivi, periodicamente verificati e aggiornati, che assicurino la 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 in materia di AML-CTF da e verso gli Organi sociali, l'Alta direzione, le strutture di controllo ed operative, il Gruppo e il Territorio;
- adozione di 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*);
- 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. Assetto organizzativo

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:

- gli Organi sociali e l'Alta Direzione che dettagliano le regole, i principi e le linee strategiche di contrasto al rischio di riciclaggio e finanziamento del terrorismo e ne dispongono le misure attuative a livello di Compagnia;
- la Funzione Antiriciclaggio il cui Responsabile svolge altresì il ruolo di Delegato per le segnalazioni delle operazioni sospette;
- i Comitati consiliari, interfunzionali e Comitato esecutivo non aziendale (Comex);
- le Funzioni aziendali di controllo, che collaborano con la Funzione Antiriciclaggio allo scopo di sviluppare metodologie condivise;



- 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;
- Comitati congiunti con le Funzioni compliance di altre società del Gruppo;
- l’Italy Compliance Committee di Territorio.

3.2.1. Organi sociali

Nelle pagine successive è riportata la descrizione dettagliata dei **compiti** e delle **responsabilità assegnate nell’ambito del modello organizzativo** adottato dalla Compagnia, ai sensi del Regolamento IVASS e in conformità al principio di “proporzionalità” e di “approccio fondato sul rischio” di cui all’articolo 4 del medesimo Regolamento.⁶

3.2.1.1. Consiglio di Amministrazione

Il Consiglio di Amministrazione di Cardif Vita (di seguito anche “CdA”), in qualità di organo di supervisione strategica, definisce le politiche aziendali (coerentemente con i principi e la regolamentazione antiriciclaggio) e individua le misure organizzative idonee a preservare l’integrità della Compagnia, nonché ad evitare il rischio di coinvolgimento in fattispecie di riciclaggio e di finanziamento al terrorismo. Più in dettaglio, il CdA in qualità di Organo di supervisione strategica adempie ai compiti ad esso assegnati dall’articolo 10 del Regolamento cui si rimanda.

3.2.1.2. Amministratore Delegato

L’Amministratore Delegato, operando nell’ambito dell’Alta Direzione, adempie ai compiti ad esso assegnati dall’articolo 11 del Regolamento cui si rimanda.

3.2.1.3. Collegio Sindacale

Il Collegio Sindacale, quale Organo di controllo vigila sull’osservanza della normativa e verifica, nel suo complesso, l’adeguatezza del sistema di gestione e controllo del rischio di riciclaggio e di finanziamento del terrorismo. In particolare, il Collegio Sindacale adempie ai compiti ad esso assegnati dall’articolo 12 del Regolamento. Cionondimeno:

- ai sensi dell’art. 46, comma 1, lettera a) del Decreto antiriciclaggio, comunica senza ritardo, al legale rappresentante o ad un suo delegato, le operazioni potenzialmente sospette di cui viene a conoscenza nell’esercizio delle proprie funzioni;
- ai sensi dell’articolo 46, comma 1, lettera b) del Decreto antiriciclaggio informa senza ritardo IVASS di tutti i fatti di cui venga a conoscenza nell’esercizio delle proprie funzioni che possano costituire violazioni gravi o ripetute o sistematiche o plurime delle disposizioni di legge e delle relative disposizioni attuative;
- ai sensi dell’articolo 51, comma 1 del Decreto antiriciclaggio riferisce entro trenta giorni al Ministero dell’economia e delle finanze, e per l’immediata comunicazione anche alla Guardia di Finanza, eventuali infrazioni alle disposizioni di cui all’articolo 49, commi 1, 5, 6, 7, 12 del medesimo Decreto.

L’informativa di cui ai punti precedenti può essere effettuata congiuntamente con altri Organi o Funzioni aziendali. A tal fine, nei confronti del Collegio Sindacale, è attivo un periodico reporting della Funzione Antiriciclaggio e del Responsabile SOS (cfr. paragrafo 3.3 “Flussi informativi e Reporting”).

3.2.1.4. Organismo di Vigilanza ex D. Lgs. n. 231/01

La Compagnia ha provveduto, mediante apposita delibera, a:

⁶ Per ogni ulteriore informazione aggiuntiva in merito al ruolo, la composizione e funzionamento degli Organi oggetto della presente descrizione si rimanda al Documento sul Sistema di Governo Societario e sul sistema di controllo interno della Compagnia, redatto ai sensi dell’art. 5 co. 2 lett. i) del Regolamento IVASS n. 38 del 3 luglio 2018.



- adottare il Modello di organizzazione, gestione e controllo (di seguito anche “Modello 231”), secondo quanto previsto dal D. Lgs. n. 231/01;
- conferire le attribuzioni ed i poteri dell’“Organismo di Controllo” ai sensi del succitato Decreto ad un organo collegiale denominato Organismo di Vigilanza (di cui tra l’altro è membro anche il Titolare della Funzione Antiriciclaggio).

Tale Organismo vigila, nell’ambito delle proprie attribuzioni e competenze ed anche in riferimento alle fattispecie di reati di riciclaggio, autoriciclaggio e finanziamento del terrorismo, richiamate da detto decreto:

- sull’osservanza del Modello da parte delle strutture interessate di Cardif Vita attraverso una costante ed indipendente azione di sorveglianza sul regolare andamento dell’operatività e dei processi di Cardif Vita al fine di prevenire o rilevare l’insorgere di comportamenti o situazioni anomale e rischiose;
- sull’efficacia ed efficienza dei processi operativi e di controllo, in relazione alle modifiche della struttura aziendale e al contesto di riferimento, nel prevenire comportamenti illeciti;
- sull’aggiornamento del Modello di Organizzazione, delle regole e dei principi organizzativi in esso contenuti o richiamati, laddove si riscontrino esigenze di adeguamento dello stesso in relazione a mutate normative, anche attraverso l’intervento dei competenti organi e funzioni societarie.

Detto Organismo accede senza limitazioni ad ogni informazione rilevante e riceve flussi informativi dalle funzioni aziendali, ai fini dell’assolvimento dei propri compiti (Cfr. paragrafo 3.3 “Flussi informativi e Reporting”).

3.2.1.5. Comitato per il Controllo Interno e i Rischi (CCIR)

L’Organo amministrativo ai sensi dell’art. 6 del Regolamento IVASS 38 del 3 luglio 2018, per l’assolvimento dei propri compiti relativi al sistema di controllo interno e gestione dei rischi, ha costituito un comitato endo-consiliare, avente funzione consultiva e propositiva nei seguenti ambiti:

- determinazione delle linee di indirizzo del sistema di controllo interno e gestione dei rischi;
- verifica periodica dell’adeguatezza e dell’effettivo funzionamento del sistema di controllo interno e gestione dei rischi;
- identificazione e gestione dei principali rischi aziendali.

Il Comitato si riunisce con frequenza almeno trimestrale ed è costituito da tre membri non esecutivi del Consiglio di Amministrazione. Oltre ai membri permanenti di cui si compone, il Comitato ha la facoltà di convocare, qualora lo ritenga opportuno, i Titolari delle Funzioni di controllo della Compagnia ed anche eventuali altri componenti del management aziendale, specialmente quelli coinvolti nelle famiglie di rischio oggetto di monitoraggio del Comitato, ivi inclusi i Presidente dell’Organismo di Vigilanza ai sensi del D. Lgs. 231/2001, il Collegio Sindacale e la Società di Revisione.

3.2.2. Strutture e Uffici posti a presidio del rischio di riciclaggio e di finanziamento del terrorismo

La Compagnia si è dotata di un assetto organizzativo che, tenuto conto della natura, della dimensione e della complessità dell’attività svolta, nonché della tipologia e della gamma dei prodotti offerti, ha l’obiettivo, tramite le funzioni di controllo e le rispettive figure chiave, di garantire l’osservanza delle norme di legge e regolamentari previste in materia di prevenzione e contrasto del riciclaggio e del finanziamento del terrorismo. In tale contesto, inoltre, svolgono un ruolo fondamentale di supporto a presidio del rischio il Comitato Antiriciclaggio, il Comitato di Sicurezza Finanziaria, il Comitato Accettazione Clienti e il Comitato KYC Review.

Al contempo, specifiche unità organizzative aziendali sono chiamate a svolgere attività connesse alla gestione del rischio di riciclaggio e contrasto al finanziamento del terrorismo.

3.2.2.1. Funzione Compliance e Funzione Antiriciclaggio

Il CdA della Compagnia ha provveduto, mediante delibera, a formalizzare l’istituzione della funzione preposta a prevenire nonché contrastare la realizzazione di operazioni di riciclaggio e finanziamento del terrorismo, denominata “Funzione Antiriciclaggio” (di seguito anche F.A.), secondo quanto previsto dall’articolo 13 del Regolamento IVASS n. 44/2019.

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 che, proprio con l'obiettivo di garantire anche a livello organizzativo quanto è già codificato nelle attribuzioni e competenze, prevede al proprio interno un'unità di Financial Security dedicata oltre che alle attività di antiriciclaggio ed antiterrorismo anche a quelle in materia di sanzioni finanziarie ed embarghi. Tale unità è articolata a sua volta in un team di "KYC & Alert Management", deputata a prevenire e contrastare la realizzazione di operazioni di riciclaggio e di finanziamento del terrorismo, principalmente attraverso lo svolgimento delle opportune attività di adeguata verifica della clientela, alla quale si affianca il team "Control & Reporting" la quale, oltre a curare gli aspetti di governance, è deputata a svolgere 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. Detta ultima struttura integra anche le attività legate alla fiscalità internazionale (normative FATCA & AEOI) e alle sanzioni internazionali/embarghi in considerazione della possibile sovrapposizione dei perimetri.

La Funzione beneficia inoltre dell'attività di supporto del team Compliance Operating and Regulatory Office che svolge attività trasversali ai diversi team della Funzione Compliance, anche relativamente agli ambiti antiriciclaggio. Il team, in particolare, fornisce supporto nella definizione della pianificazione delle attività, nella raccolta dei fabbisogni formativi e nella rendicontazione verso gli Organi Societari, l'Alta Direzione 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.

Il Titolare della Funzione Antiriciclaggio coincide con il Responsabile della Funzione Compliance nell'ottica e con la finalità di poter agevolare ogni utile individuazione delle normative e della conformità nell'applicazione delle stesse, rispetto alle disposizioni e/ o regole e/ o principi di Gruppo e/o locali. Il Titolare della Funzione Antiriciclaggio è stato nominato dal Consiglio di Amministrazione del 26 marzo 2012 da ultimo confermato nel ruolo nella seduta del 28 settembre 2021. Il medesimo Titolare della Funzione Antiriciclaggio ricopre altresì il ruolo di Delegato per la segnalazione delle operazioni sospette.

Il Responsabile della Funzione Antiriciclaggio risponde direttamente al Consiglio di Amministrazione.

La F.A. è preposta al presidio e al controllo della conformità della Compagnia alle prescrizioni contenute nelle norme di legge, nelle disposizioni regolamentari, nei codici di comportamento e nelle regole interne in materia di antiriciclaggio.

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 stessa 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 al Consiglio di Amministrazione, al Collegio Sindacale e all'Organismo di Vigilanza sull'attività svolta, sulle verifiche effettuate e sulle eventuali raccomandazioni formulate; inoltre, la Funzione informa regolarmente l'Alta Direzione e 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 il Responsabile Antiriciclaggio o suo delegato.

A tal fine, la Funzione Antiriciclaggio svolge i seguenti compiti:

- identifica le regole applicabili sotto il profilo della classificazione del rischio di riciclaggio coerentemente con la politica di gestione del rischio di Gruppo e della Compagnia, secondo i criteri tempo per tempo prestabiliti: - ad oggi — clientela, prodotti, tipologia di transazioni, canali distributivi utilizzati e Paese di origine o residenza, valutandone l'impatto sui processi e le procedure interne (anche a seguito delle risultanze dei controlli effettuati);
- collabora all'individuazione degli assetti organizzativi finalizzati alla prevenzione e al contrasto dei "rischi" antiriciclaggio e finanziamento del terrorismo e ne verifica, nel continuo, il loro grado di efficienza ed efficacia, suggerendo le modifiche, opportune e necessarie al Consiglio di Amministrazione con ponderazione delle "criticità" riscontrate e attraverso una declinazione del rischio Compagnia (oltre che di rischio Cliente). A tal fine, verifica nel

continuo l'idoneità dei modelli organizzativi adottati e propone eventuali modifiche strutturali e procedurali necessarie al contenimento del rischio, anche nei confronti di intermediari e outsourcers;

- concorre a diffondere all'interno della Compagnia la cultura in materia di antiriciclaggio ed antiterrorismo.

Con riferimento alle relazioni con l'Alta Direzione, il Consiglio di Amministrazione, il Collegio Sindacale e le altre Funzioni di Controllo:

- presenta – annualmente e comunque in caso di significative modifiche o anche di un andamento incrementale o anche su alcune attività, prodotti, o altri *driver* del rischio cui l'impresa è esposta – agli Organi aziendali una relazione i. sulle attività svolte e le verifiche compiute, ii. Sulle valutazioni effettuate, iii. Sulle criticità e carenze rilevate o ambiti di miglioramento, iv. Sulle raccomandazioni formulate per la loro rimozione, nonché sullo stato e sui tempi di implementazione degli interventi migliorativi, qualora non ancora realizzati, v. sull'attività formativa, vi. Sui risultati dell'esercizio di autovalutazione condotto ai sensi delle disposizioni sulle procedure di mitigazione del rischio, vii. Il piano delle azioni correttive ancora da intraprendere, tenuto conto delle carenze riscontrate nelle verifiche precedenti e di eventuali nuovi rischi identificati;
- concorre a predisporre e aggiornare gli orientamenti strategici e la “metodologia di gestione e classificazione del rischio di riciclaggio e di finanziamento del terrorismo” da sottoporre a validazione da parte dell'Organo Amministrativo e la politica aziendale riportante le scelte rilevanti in materia di assetti organizzativi, procedure e controlli interni, conservazione dei dati e adeguata verifica, nonché contribuisce a tenere aggiornato il “documento analitico” aziendale;
- predispone per il Consiglio di Amministrazione, per il Collegio Sindacale e per l'Organismo di Vigilanza ex D. Lgs. n. 231/01 le relazioni periodiche riguardanti la materia antiriciclaggio/antiterrorismo, altresì, evidenziando eventuali criticità che possano esplicitare effetti circa la tenuta dei “protocolli” e/o delle regole di condotta a contrasto del rischio di riciclaggio in coerenza con il Modello Organizzativo e di Gestione ex D. Lgs. n. 231/01;
- provvede a fornire tempestivamente informativa agli Organi Aziendali in caso di disfunzioni gravi o in presenza di una criticità rilevante, proponendo le azioni correttive da intraprendere, con le relative azioni al fine di evitare il ripetersi della criticità;
- informa regolarmente l'Alta Direzione e 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 il responsabile antiriciclaggio è membro permanente o periodicamente invitato.

Con riferimento alle Relazioni con il Mestiere, il Territorio ed il Gruppo:

- provvede a segnalare tempestivamente alle strutture di Compliance superiori le principali nuove norme e le conseguenti necessarie implementazioni da apportare ai processi e alle procedure e agli strumenti tecnici o database aziendali, le eventuali gravi criticità in tema di conformità riscontrate nell'ambito della propria attività, nonché fornisce reporting periodici circa le attività svolte (KPRI – Key Performance Risk Indicators -);
- partecipa ad eventuali comitati territoriali in materia.

Con riferimento alle Relazioni con le Autorità di Vigilanza:

collabora con le Autorità, fornendo ogni informazione o reportistica richiesta sia specificamente alla Compagnia che per il tramite di lettere/provvedimenti indirizzati all'intero mercato;

- trasmette mensilmente all'UIF (Unità di Informazione Finanziaria) i dati aggregati (c.d. segnalazioni S.Ar.A.), verificando preventivamente, in coordinamento con l'ufficio Regulatory Controls, secondo le risultanze trasmesse dalla stessa Autorità, l'attendibilità del dato con le registrazioni effettuate e l'operatività stessa, nonché esamina e riscontra le comunicazioni dell'Autorità di Vigilanza circa eventuali anomalie statistiche o altri rilievi.

Con riferimento all'attività di Advisory:

- garantisce l'ottemperanza, nell'espletamento delle attività assicurative, degli obblighi relativi alle materie di propria competenza, anche promuovendo i progetti relativi all'antiriciclaggio/antiterrorismo, nonché partecipando per la parte di competenza ai più generali progetti aziendali;
- svolge l'attività di c.d. “legal watch”, che consiste principalmente nell'intercettare la nuova normativa in materia di antiriciclaggio e finanziamento del terrorismo potenzialmente applicabile alla Compagnia in base alla sua operatività.



In caso di mutamenti del quadro normativo, la Funzione Antiriciclaggio effettua le relative analisi d'impatto sui processi e sulle procedure interne;

- presta la propria assistenza specialistica alle altre funzioni, agli Organi aziendali, nonché all'Alta Direzione della Compagnia, a supporto dell'evasione di ogni tematica e/o attività e/o prodotto che sia considerato a potenziale rischio di riciclaggio, al fine di individuare preventivamente idonei presidi di contrasto e controllo.

Con riferimento alle attività di Risk Assessment:

- predispone i contenuti della metodologia di rischio e svolge l'autovalutazione prevista dalla regolamentazione IVASS, aggiornandone i processi, gli adempimenti e ogni altra attività, in coerenza con le risultanze;
- effettua regolarmente delle attività di Risk Assessment, sia in base alla normativa locale (Autovalutazione⁷) che ad indicazioni di Gruppo con l'obiettivo di effettuare la valutazione dei rischi intrinseci e residuali in ambito antiriciclaggio, anche al fine di individuare da un lato le principali aree di miglioramento delle proprie attività, dall'altro i processi da sottoporre a verifica.

Con riferimento alle attività di controllo:

- 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, che comprende altresì i controlli di II livello sulla Funzione stessa sotto il coordinamento del Compliance Risk & Control Manager di Head Office;
- 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 primo livello eseguiti dalle funzioni operative;
- verifica la corretta conservazione dei dati necessari per le valutazioni ai fini antiriciclaggio e antiterrorismo;
- verifica, sotto il profilo operativo, l'effettiva applicazione delle procedure antiriciclaggio e antiterrorismo, in particolare relative a: "adeguata verifica"; "conservazione/registrazione e conservazione dei dati", "rilevazione, valutazione e segnalazione di operazioni sospette", effettivo riscontro verso le liste di sorveglianza a contrasto del finanziamento del terrorismo, individuandone (eventuali) potenziali criticità, al fine di suggerire le misure correttive;
- effettua attività di controllo periodico nei confronti degli Intermediari e degli outsourcers ai quali la Compagnia ha conferito delega ad effettuare, in proprio nome e conto, l'attuazione degli adempimenti previsti dalla normativa antiriciclaggio;
- riporta periodicamente 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.

Con riferimento all'attività di aggiornamento di politiche e procedure:

- collabora alla definizione delle politiche di governo del rischio di riciclaggio e delle varie fasi in cui si articola il processo di gestione del rischio di riciclaggio;
- contribuisce alla revisione e all'aggiornamento, delle policy e delle procedure di propria competenza, sia adeguando le stesse alle nuove normative e/o disposizioni regolamentari, sia anche attraverso la verifica di applicabilità comparata con le policies e le procedure emanate dal Gruppo e dalla struttura di Head Office;
- valida e/o integra, ove necessario, le procedure di competenza delle altre Funzioni Aziendali con eventuali impatti antiriciclaggio/antiterrorismo.

Con riferimento all'attività di formazione:

- concorre a diffondere la cultura in materia di antiriciclaggio/antiterrorismo, promuovendo adeguate attività formative dedicate a tutto il personale e ai propri collaboratori;
- attraverso la redazione di idonee istruzioni e linee guida dedicate, che tengano conto delle caratteristiche dei prodotti commercializzati, collabora nell'assicurare che gli Intermediari costituenti la rete distributiva diretta siano sempre a conoscenza delle procedure ai fini del corretto adempimento degli obblighi antiriciclaggio e antiterrorismo.

Con riferimento all'attività di adeguata verifica:

⁷ Si veda sez. VI del Reg. IVASS 44/2019 così come modificata dal Prov. IVASS 111/2021.

- 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.
- valuta l'adeguatezza dei sistemi informativi e delle procedure interne volti a: i. all'adempimento degli obblighi di adeguata verifica della clientela; ii. Alla rilevazione, valutazione e segnalazione delle operazioni sospette, iii. Alla rilevazione delle ulteriori situazioni oggetto di obbligo di comunicazione; iv. Alla conservazione dei documenti, dati e informazioni richiesti dalla normativa; v. alla predisposizione di ogni utile misura, oltre che ad integrazione dell'acquisizione di dati sul reddito e sul patrimonio, anche circa l'accertamento dell'origine dei fondi;
- applica misure rafforzate di adeguata verifica della clientela nei casi in cui appaia particolarmente elevato il rischio di riciclaggio;
- individua le fattispecie nonché le regole, le procedure e i "format" utili per acquisire i dati, i documenti e le informazioni necessarie ad assolvere alla "adeguata verifica rafforzata", inclusa ogni misura di accesso immediato o tempestivo (anche per fornire riscontro o consentire l'accesso alle Autorità competenti);
- cura, in ogni caso, l'istruttoria per la segnalazione di operazioni sospette inoltrate dai responsabili delle unità organizzative che gestiscono i rapporti con la clientela e dagli intermediari assicurativi;
- valuta ogni e opportuna misura di applicazione dell'obbligo di astensione, così come previste dalla Legge e/o dalle disposizioni aziendali o di Gruppo ove più stringenti, curandone l'indicazione dei principi e delle regole da rispettare sia in fase assuntiva sia in fase post-vendita.

Con riferimento al sistema di allerta etico antiriciclaggio (whistleblowing):

- partecipa al processo di implementazione, quindi, di valutazione del sistema di "allerta etico/whistleblowing" in ambito sicurezza finanziaria, a tal fine raccordandosi e cooperando con ogni altra entità di controllo anche di Gruppo.

Con riferimento all'accettazione e monitoraggio di intermediari e fornitori;

- partecipa al processo di accettazione e di revisione degli intermediari e dei fornitori/outsourcer nella valutazione, nel monitoraggio periodico ed aggiornamento del profilo di rischio con riferimento alle tematiche dell'antiriciclaggio/antiterrorismo, secondo i principi del modello di analisi dei rischi adottato dalla Compagnia conformemente, ove applicabile, alla classificazione dei rischi del Gruppo Bnp Paribas.

Con riferimento ai prodotti:

- analizza, nella fase di definizione dei nuovi prodotti e in via preventiva rispetto alla commercializzazione degli stessi, gli aspetti antiriciclaggio e antiterrorismo ad essi connessi predisponendone il relativo assetto dei controlli, a tal fine fornendone validazione per la parte di competenza;
- svolge attività di controllo e di advisory sui prodotti già commercializzati avendone funzione di consultazione preventiva e di indicazione delle misure da implementare per la conformità dei prodotti;
- collabora nelle attività di predisposizione delle clausole standard da inserire all'interno della documentazione contrattuale di prodotto e nei relativi accordi distributivi ivi compresi eventuali Service Level Agreement, nonché della modulistica per i clienti con riferimento agli aspetti di antiriciclaggio e antiterrorismo.

Con riferimento alla gestione di richieste nominative, gestione liste e controlli antiterrorismo – sanzioni finanziarie:

- analizza costantemente gli esiti delle verifiche riguardanti le liste nominative di sorveglianza a contrasto del finanziamento del terrorismo e individua le regole per l'impostazione dei "blocchi" procedurali in raccordo con le restrizioni all'operatività internazionale in materia di contrasto di finanziamento del terrorismo, alle sanzioni finanziarie/embarghi e/o ad ogni altra limitazione applicabile
- redige puntuale e tempestiva risposta (sia positiva sia negativa) alle richieste di informazioni inviate dall'Autorità di Vigilanza o Giudiziaria, in materia di antiterrorismo ed antiriciclaggio. Nei casi di riscontro "positivo" ne valuta, attraverso apposite analisi, gli effetti sul "rischio cliente".

Con riferimento alle analisi ed invio di:

- (a) rapporti/operazioni anomale (passibili di divenire sospette), analizza le posizioni “anomale”, qualificabili come potenzialmente “sospette” generate dalla piattaforma informatica adottata dalla Compagnia e provenienti da segnalazioni nell’ambito del processo di escalation svolto dal I Livello, dagli Organi di controllo della Compagnia, dal Gruppo e da Autorità di controllo esterne. A tal fine, coopera e supporta il Delegato per le segnalazioni delle operazioni sospette nella fase di analisi istruttoria e di acquisizione e valutazione di ogni evento di rischio al fine di procedere all’invio all’Autorità (UIF) secondo gli standard previsti dalla normativa vigente. Collabora all’aggiornamento delle regole da utilizzarsi nei software per la rilevazione delle anomalie, ponendo specifico riferimento e attenzione al rispetto della prevenzione/anticipazione anche quale assolvimento della segnalazione rispetto al compimento dell’operazione. Valuta l’adeguatezza degli strumenti di rilevazione assicurando che le soglie ed i criteri applicati siano coerenti ai rischi individuati a livello locale ed ai regolamenti applicabili. Valuta e rende ogni misura, istruzione o parere circa l’applicazione di misure di astensione in conformità alla Legge, tempo per tempo, vigente;

Con riferimento ai rapporti con la “rete distributiva diretta”:

- partecipa al processo di redazione di apposite Circolari dispositive/informative e/o istruzioni operative da inviare agli Intermediari costituenti la Rete Distributiva diretta della Compagnia, richiamando nell’ambito di tali comunicazioni, le regole di comportamento ai fini del contrasto al riciclaggio ed al finanziamento del terrorismo cui gli stessi Intermediari devono attenersi nell’esercizio della propria attività;
- predispone, ove necessario, procedure organizzative ed anche i livelli di servizio attesi o necessari (cd. Service Level Agreement) con i principali intermediari, nonché specifiche clausole nell’ambito dei contratti di collocamento e/o distribuzione;
- predispone congiuntamente agli intermediari idoneo materiale e/o istruzioni a supporto della formazione;
- effettua una valutazione sul puntuale assolvimento delle regole della Compagnia e/o di esposizione al rischio degli Intermediari facenti parte della Rete Distributiva Diretta;
- svolge incontri periodici con cadenza regolare con i principali distributori con l’obiettivo di condividere i temi legati all’Antiriciclaggio ed alle sue connessioni ai processi e ai controlli di business.

3.2.2.2. Responsabile della Funzione Antiriciclaggio e Responsabile / Delegato per le segnalazioni delle operazioni sospette (SOS)

La Compagnia, in relazione alla propria struttura ed alla ravvisata esigenza di meglio ponderare ogni attività segnaletica in relazione al “rischio di riciclaggio”, ha provveduto mediante apposita delibera del CdA, a nominare l’attuale Responsabile della Funzione Compliance quale Responsabile della Funzione Antiriciclaggio e Delegato SOS.

Il Titolare della Funzione Antiriciclaggio è nominato e revocato dal CdA, secondo procedure di selezione formalizzate nella “Politica Antiriciclaggio” e rispetta i requisiti di onorabilità, professionalità e indipendenza.

A presidio della stabilità e dell’indipendenza del Titolare della Funzione, è previsto che riferisca direttamente, per gli ambiti definiti dalle disposizioni regolamentari, al Consiglio di Amministrazione.

Il Responsabile/Delegato SOS:

- valuta – sulla base delle istruzioni, schemi e degli indicatori di anomalia emanati dalla UIF, nonché alla luce di tutti gli elementi disponibili, acquisiti anche tramite le strutture di primo livello e gli intermediari assicurativi – le operazioni sospette comunicate dal responsabile di qualsiasi unità organizzativa dell’impresa e dell’intermediario assicurativo, ovvero di cui sia altrimenti venuto a conoscenza nell’ambito della propria attività, acquisendo ulteriori informazioni tramite le strutture di primo livello, gli intermediari assicurativi o altre fonti liberamente accessibili;
- esamina e trasmette alla UIF le segnalazioni di operazioni sospette ritenute fondate attribuendo una valutazione di rischio coerente con le risultanze delle motivazioni addotte, anche consentendo all’Autorità stessa, in dipendenza del rischio, di attuare misure cautelari di sospensione ex art. 6 comma 4 D. Lgs. n. 231/07 e s.m.i.;
- esamina e trasmette per l’archiviazione in apposito dossier/modalità riservata le anomalie che non siano valutate come passibili di segnalazione all’Autorità competente, effettuando ogni necessaria misura e/o apportando ogni motivazione idonea sia essa specifica sia generale (i.e. per tipologie di anomalie esaminate che abbiano a fondamento dell’archiviazione una motivazione simile o identica);



- predispone, anche nella sua qualità di Responsabile della Funzione Antiriciclaggio, ogni opportuna misura, organizzativa, informatica e di conferimento di istruzioni al personale e/o predisposizione di appropriati controlli, al fine di modificare e/o integrare e aggiornare le regole e/o gli eventi di rischio;
- effettua in modalità coerente con i rischi individuati, valutati e segnalati ogni pertinente valutazione circa l'applicazione dell'obbligo di astensione e il raccordo con l'innalzamento o il decrescere del rischio associato al cliente;
- effettua ogni attività dipendente, correlata e/o conseguente alla valutazione e segnalazione di operazioni sospette, raccordandosi e cooperando con le Autorità competenti (i.e. UIF ma anche Magistratura Ordinaria e/o Guardia di Finanza);
- effettua verifiche, anche a campione, in raccordo con la Funzione Antiriciclaggio e Internal Audit, sulla congruità delle valutazioni di primo livello svolte sull'operatività della clientela dalle strutture dell'impresa o dall'intermediario assicurativo;
- comunica, con modalità idonee a garantire la tutela della riservatezza anche nei confronti degli esponenti e delle altre funzioni aziendali non coinvolte nel processo di segnalazione: a) l'esito della propria valutazione al responsabile dell'unità organizzativa dell'impresa o alla Funzione Antiriciclaggio dell'intermediario assicurativo che hanno effettuato la segnalazione, impiegando modalità organizzative che ne consentano la tracciabilità; b) i nominativi dei clienti oggetto di segnalazione di operazioni sospette ai responsabili delle strutture competenti ai fini dell'attribuzione o dell'aggiornamento del profilo di rischio dei clienti stessi, nonché all'intermediario assicurativo che ha distribuito il relativo contratto.

Inoltre, il responsabile per la segnalazione delle operazioni sospette ha libero accesso ai flussi informativi diretti agli organi aziendali ed alle strutture coinvolte nella gestione e nel contrasto del rischio di riciclaggio. Il responsabile per la segnalazione delle operazioni sospette ha il compito di intrattenere rapporti con la UIF e di rispondere tempestivamente ad eventuali richieste formulate dalla stessa unità.

3.2.2.3. Regulatory Controls

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/ CFT.

Con riferimento al presidio di I livello, assumono, inoltre, valenza fondamentale i controlli di linea integrati nelle procedure informatiche, che comportano blocchi, sospensive, elaborazioni e verifica dell'esistenza di autorizzazioni automatiche (connesse al verificarsi di determinati eventi e di pre-individuate istruzioni) volte a garantire il corretto svolgimento delle attività.

L'unità "Regulatory Controls", a supporto della Funzione Antiriciclaggio:

- gestisce il processo per l'analisi di *due diligence* dei clienti sulla base dei criteri stabiliti dalle relative procedure;
- effettua l'analisi dei *dossier* ad alto rischio 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 (in quest'ultimo caso in seguito alle specifiche richieste veicolate dalla Funzione Antiriciclaggio);
- 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;
- 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.

3.2.2.4. Internal Audit

La Funzione di revisione interna denominata "Internal Audit" è responsabile dello svolgimento dei controlli di III livello e, in conseguenza dell'attività svolta, contribuisce quindi a garantire l'adeguatezza del sistema antiriciclaggio nel suo complesso. In particolare, tale funzione verifica, attraverso dedicati controlli periodici:

- il dispositivo di *governance*, gestione dei rischi e controllo interno in materia di antiriciclaggio;
- il costante rispetto dell'obbligo 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, 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, l'alta direzione 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.

3.2.2.5. Risk Management

La Funzione di Risk Management assicura il presidio e l'adeguata implementazione del sistema della gestione dei rischi della Compagnia, anche con riferimento ai rischi di riciclaggio e finanziamento del terrorismo, nel rispetto della regolamentazione esistente e delle *guidelines* di Gruppo, concorrendo alla mappatura dei rischi aziendali, alla loro valutazione anche prospettica e misurazione anche in presenza di scenari stressati ed al relativo reporting. In tale ruolo, detta funzione contribuisce allo sviluppo della cultura del rischio ed all'introduzione di una logica "*risk based*" integrata nei principali processi aziendali. In ottica di indipendenza della funzione di controllo, il Responsabile Risk Management è alle dirette dipendenze del Consiglio di Amministrazione che ha accesso diretto e senza restrizioni alle attività della funzione.

In particolare, la Funzione di Risk Management assicura l'identificazione, l'analisi e la misurazione dei rischi operativi, in coerenza con le metodologie definite a livello aziendale. Durante il Comitato Rischi vengono forniti i piani ed i dettagli del GRP da parte della funzione Customer Service.

Con specifico riferimento alle attività di reporting:

- predispone periodicamente la reportistica sull'evoluzione dei rischi e la violazione dei limiti operativi che rientrano nella sua area di responsabilità e ne condivide i risultati con l'Organo Amministrativo, l'Alta Direzione ed i responsabili delle strutture operative garantendo se necessario anche adeguato processo di *escalation*;

- analizza la reportistica sull'evoluzione dei rischi e la violazione dei limiti operativi predisposta dalle altre aree coinvolte, ivi inclusa la Funzione Antiriciclaggio, garantendo se necessario anche adeguato processo di *escalation*;
- effettua le comunicazioni relative alle esternalizzazioni delle funzioni essenziali o delle attività importanti nei termini previsti dal Reg. 38/2018;
- predispone in particolare un monitoraggio periodico delle Metriche di Rischio con l'obiettivo di quantificare le esposizioni ai principali rischi a cui è esposta la Compagnia ed informare periodicamente l'Alta Direzione e l'Organo Amministrativo.

La Funzione di Risk Management, inoltre, con riferimento ai Comitati, tra gli altri organizza con periodicità trimestrale, il Comitato Rischi Operativo della Compagnia.

3.2.2.6. Altre 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 struttura 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 competenza⁸:

- 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.
- Process Engineering cura lo sviluppo e l'implementazione di metodologie e di strumenti per il disegno / revisione dei processi aziendali, supportando tutte le funzioni aziendali. Si occupa, inoltre, con riferimento alle iniziative rilevanti / strategiche di competenza, il 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 altre unità aziendali, il corretto dimensionamento delle unità organizzative.
- 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 da Internal Audit, 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.

⁸ Al fine di fornire una visione quanto più esaustiva e completa delle Unità Organizzative e del loro coinvolgimento nelle attività connesse alla gestione del rischio di riciclaggio e finanziamento del terrorismo, al presente paragrafo si riporta altresì la descrizione di Unità Organizzative già definite in ulteriori paragrafi del presente Documento a cui si rimanda per gli ulteriori dettagli e specifiche non già ricomprese alla presente sezione.

- 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 Local Conduct Referent, 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 struttura 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 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 e identificando e coordinando gli interventi di adeguamento o le azioni correttive individuate nello svolgimento delle attività di competenza.

3.2.3. Comitati a presidio del rischio di riciclaggio e di finanziamento del terrorismo

3.2.3.1. Comitato Antiriciclaggio

Il "Comitato antiriciclaggio" analizza le operazioni presentate e già previamente istruite dalla Funzione Antiriciclaggio, in coerenza con i rischi individuati e 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, ovvero mancato rispetto delle sanzioni finanziarie.

Fermo il rispetto dell'assolvimento segnaletico con immediatezza e, comunque, prima del compimento dell'operazione, qualora si ravvisasse la necessità di un confronto per le operazioni ritenute potenzialmente sospette, il Comitato Antiriciclaggio assolve ad una funzione di carattere consultivo nei confronti del Delegato per le Segnalazioni di operazioni sospette, senza pregiudizio alcuno delle attribuzioni del Delegato SOS che può assumere ogni decisione finale circa l'assolvimento dell'obbligo segnaletico (e correlate misure, ivi inclusa l'astensione o il congelamento o la proposizione per la risoluzione del rapporto), in maniera autonoma.

I partecipanti al Comitato sono:

- Delegato SOS / Titolare della Funzione Antiriciclaggio;
- coordinatore dell'Ufficio Financial Security;
- coordinatore del team KYC & Alert Management;
- analista senior della Funzione Antiriciclaggio che ha preso in carico l'analisi della/delle operazione/i sospetta/e;
- ogni altra Funzione e/o soggetto che, in ragione della tipologia di rischio (nella propria declinazione di rapporto, prodotto, cliente, operazione; Paese) possa risultare utile o necessario coinvolgere nella valutazione.

Il Comitato si riunisce ogniqualvolta vi sia necessità di sottoporre un dossier all'attenzione del Delegato SOS.

A seguito dell'analisi effettuata, possono essere assunte le seguenti decisioni:

- segnalazione all'UIF ai sensi dell'art. 35 D. Lgs. n. 231/07;
- condivisione del rischio con le altre Società del Gruppo Assicurativo e/o del Gruppo BNPP;
- richiesta di sospensione (ex art. 6 co. 7 D. Lgs. cit.) all'U.I.F.;
- asset freeze sul nominativo al fine di monitorare la pozione;
- ogni determinazione afferente a modifiche suggerite ai prodotti, alle modalità di instaurazione dei rapporti e/o qualsiasi altra determinazione connessa al contenimento di un rischio sistemico;
- la non applicabilità/non necessità di adozione di misure specifiche e/o integrative rispetto ai presidi in essere.

Le riunioni del Comitato sono opportunamente documentate attraverso la redazione di un verbale al fine di poter tenere adeguata “tracciabilità” dell’iter logico delle determinazioni ed anche dei documenti acquisiti e della istruttoria effettuata.

3.2.3.2. Comitato di Sicurezza Finanziaria

Il “Comitato di sicurezza finanziaria”, ha lo scopo di:

- supervisionare nel tempo le attività aziendali poste in essere per la conformità alle disposizioni previste dalle normative antiriciclaggio, antiterrorismo, di conformità con le sanzioni finanziarie e con la fiscalità internazionale (i.e. FATCA ed AEOI), fornendo supporto sulle questioni di rilevanza e su tutte quelle tematiche che superano l’ordinaria gestione degli adempimenti previsti dalla relativa normativa di riferimento, fornendo indicazioni di indirizzo strategico e valutando, quando necessario, le azioni da intraprendere per quanto concerne la corretta risoluzione delle criticità e/o delle problematiche;
- analizzare le anomalie e le criticità riscontrate durante l’attività condotta dalla Funzione Antiriciclaggio, anche rinvenienti da attività di controllo di II livello, nonché valutare le relative indicazioni/ proposte di adeguamento e le azioni correttive individuate;
- analizzare le criticità e le carenze rilevate;
- condividere le raccomandazioni formulate per la loro rimozione, nonché lo stato e i tempi di implementazione degli interventi migliorativi, qualora non ancora realizzati;
- analizzare il piano delle azioni correttive ancora da intraprendere, tenuto conto delle carenze riscontrate nelle verifiche precedenti e di eventuali nuovi rischi identificati;
- 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.

I partecipanti al Comitato sono, in qualità di membri permanenti:

- Responsabile Compliance / Antiriciclaggio;
- Chief Operating Officer o un suo delegato;
- Responsabile Customer Service;
- Responsabile Operations Controls e/o un suo delegato;
- Coordinatore dell’Ufficio Financial Security;
- Coordinatori dei team KYC & Alert Management e Control & Reporting.

Altri partecipanti, su invito di un membro permanente e sulla base di specifiche tematiche (anche allorquando si renda necessario o opportuna la loro partecipazione ove si trattino tematiche che possano avere un impatto trasversale o distributivo o di prodotto, come tale non limitato al caso di specie).

Nei confronti di tali partecipanti, permane fermo l’obbligo di riservatezza e, in specie, in dipendenza della determinazione da assumere, la loro partecipazione può avvenire ai fini della disamina della fattispecie e del rischio sottostante, quindi, anche senza alcuna *disclosure* del nominativo del Cliente passibile di segnalazione.

Il Comitato è convocato dalla Funzione Antiriciclaggio con periodicità trimestrale che può variare a seconda delle effettive esigenze intervenute. Le riunioni del Comitato sono documentate da un verbale redatto dal Coordinatore dell’Ufficio Financial Security ed inviato ai partecipanti.

3.2.3.3. Comitato Accettazione Clienti e KYC Review

Il Comitato Accettazione Clienti (CAC) e il Comitato KYC Review (KYC review) sono misure rafforzate di *due diligence*. Il loro scopo è quello di sottoporre all’Alta Direzione (ovvero ad altri soggetti appositamente delegati o che svolgono funzioni equivalenti), al Business e 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.

La sottoposizione dei *dossier* della clientela ad un Comitato ha la funzione di condividere l’analisi del rischio sotto più profili. Ciò in quanto consente sia di effettuare analisi complete e adeguate, sia di fornire un supporto istruttorio e probatorio ai membri del Comitato che dovranno effettuare la determinazione finale.

La Compagnia ha ritenuto opportuno estendere il livello decisionale più alto (rappresentato dal CAC) a tutti i casi di relazioni individuate come ad “alto rischio”⁹, a prescindere dalla possibilità, concessa dai requisiti di Gruppo (si confronti la Know Your Client – Global Policy), di differenziare tra CAC e BU Management & Compliance (B&C) a seconda delle caratteristiche della posizione sottoposta a valutazione. In tale ottica, i comitati locali CAC e KYC Review sono composti dai medesimi membri e si distinguono per quanto segue:

- il CAC è convocato per decidere sull’entrata in relazione;
- il KYC Review è convocato in caso di ricertificazione programmata, innalzamento del profilo di rischio, nonché in presenza di ogni altro evento o notizia che abbia un impatto sul profilo di rischio di una relazione esistente.

Il processo decisionale formalizzato dai Comitati anzidetti dovrà comunque tenere in considerazione, laddove necessario (ad esempio in relazione alla frequenza di ricertificazione), la segmentazione della clientela e la categoria relativi al *dossier*, come previsto all’interno del c.d. KYC Compendium di Gruppo.

Di seguito vengono rappresentati i membri permanenti dei due Comitati:

- il Responsabile della Compagnia o il Co-general Manager (se presente) o loro delegati – in qualità di presidente del Comitato;
- il Responsabile Relationship Manager (“RM”) o suo delegato, accompagnato dal RM responsabile della pratica del cliente ove applicabile;
- Il Responsabile della Funzione Antiriciclaggio, accompagnato dal membro della Funzione Antiriciclaggio incaricato della revisione del *dossier* se diverso.

I membri permanenti possono invitare altri partecipanti come:

- il Responsabile del Risk o suo delegato;
- il Responsabile del Legale o suo delegato;
- il responsabile delle attività di Corporate Social Responsibility (“CSR”) della Compagnia;
- ogni altro partecipante laddove richiesto da un membro permanente.

Le riunioni dei Comitati possono essere tenute anche tramite le modalità ritenute opportune a garantire ed agevolare l’efficienza degli incontri (i.e. via email, da remoto). In questo caso le autorizzazioni saranno fornite con mail e conseguentemente archiviate.

La Funzione Antiriciclaggio può sempre richiedere al segretario del Comitato che venga convocato un CAC o un KYC Review ogni volta che sia ritenuto opportuno. Le informazioni e le analisi di base devono essere diffuse prima del processo CAC e KYC Review, con documentazione di supporto ove rilevante.

Il Segretario dei Comitati è il KYC Operations Manager o qualsiasi altra persona nominata dal *Business*. A livello locale, la figura del KYC Operations Manager¹⁰ è da ricondurre al Responsabile Regulatory Controls in qualità di titolare dell’ufficio dedicato alla gestione dei processi KYC della Compagnia ed è responsabile di:

- stabilire le modalità di svolgimento delle riunioni, assicurando la partecipazione dei membri dei Comitati, definendo l'ordine del giorno e fornendo la documentazione rilevante prima delle riunioni;
- annotare le presenze e le decisioni e provvedere alla verbalizzazione delle riunioni;
- tenere traccia delle condizioni stabilite dai Comitati e rendere informativa agli stessi quando le medesime condizioni vengono soddisfatte, o laddove non venissero soddisfatte entro il termine stabilito;
- provvedere all'*escalation* del *dossier* al livello appropriato quando richiesto.

3.2.3.4. Comitato Accettazione Intermediari (IAC)

Il Comitato di Accettazione degli Intermediari (IAC) è una misura di due diligence rafforzata che ha lo scopo di sottoporre all’Alta Direzione, oltre che alla Funzione Compliance, i rapporti commerciali nuovi ed esistenti che presentano un rischio alto (High Risk level) sulla base delle analisi condotte. Il Comitato si riunisce anche nei casi in cui la due diligence condotta

⁹In accordo con l’esenzione validata dal Polo e da KYC *domain* “Decision making rules” formalizzata nel file EP nr. 124429, Cardif Vita applica il principio di *reliance* sul *Primary Site* (ovvero BNL) per una serie di relazioni con la clientela, tra cui quelle a “rischio basso” e a “rischio medio”. In particolare, l’esenzione stabilisce l’accettazione automatica delle relazioni a perimetro senza che sia necessaria l’applicazione dell’autonomo processo decisionale di Cardif (descritto nel presente documento).

¹⁰ Per lo svolgimento delle attività del KYC Operations Manager è prevista, inoltre, la possibilità di delega previa approvazione del *Business*.

abbia rilevato la presenza (i) dell'intermediario nelle liste CSR (Corporate Social Responsibility), (ii) nella compagine sociale di PEP in qualità di UBO (Ultimate Beneficial Owner), SMO (Senior Managing Officials), (iii) esercenti l'attività in qualità di persone fisiche (c.d. Individual Intermediary).

Il comitato IAC può essere convocato su richiesta o in caso di obiezione da parte di Compliance sia in caso di accettazione che di ricertificazione di un Intermediario.

L'attività del Comitato si basa sulla valutazione dei potenziali rischi connessi all'entrata in relazione stessa o al mantenimento della relazione esistente (rischio reputazionale, rischio finanziario, rischi specifici nell'ambito della Financial Security, rischio regolamentare e sanzionatorio, protezione degli interessi dei clienti, rispetto delle regole di etica professionale, eccetera).

I partecipanti sono:

- Il Responsabile della Compagnia o suo delegato, presidente del Comitato IAC (ruolo svolto dall'Amministratore Delegato o suo delegato per Cardif Vita S.p.A.);
- Il Responsabile Partnership o il Responsabile Coverage (identificato nella funzione Commercial Direction) o suo delegato, accompagnato dal Relationship Manager incaricato del fascicolo dell'Intermediario, ove applicabile;
- Il Responsabile Compliance, o suo delegato appartenente all'Ufficio Financial Security, accompagnato dal membro di Compliance incaricato della revisione del fascicolo, se persona diversa.
- Il KYI Operation Manager (identificato nella funzione Operational Permanent Control) in qualità di Segretario. Il Segretario redige il verbale del Comitato.

Possono inoltre essere invitati:

- Il Responsabile del Risk (identificato nella funzione Risk Management), o persona delegata;
- Il Responsabile del Legal (identificato nella funzione Legal & Corporate Affairs), o persona delegata;
- Il rappresentante CSR (identificato nel Responsabile della funzione Communication Media & CSR);
- Qualunque altro partecipante richiesto da un membro permanente.

Le riunioni del Comitato sono documentate da un verbale redatto dalla funzione Operational Permanent Control, in qualità di Segretario ed inviato ai partecipanti.

3.3. Flussi informativi e reporting

Al fine di presidiare il rischio di riciclaggio e finanziamento del terrorismo, i vari organi sociali, le funzioni di controllo, e le strutture organizzative predispongono e ricevono flussi informativi (e.g. report, comunicazioni, segnalazioni etc.) dai diversi soggetti sia interni che esterni all'impresa.

Si fornisce evidenza, nelle tabelle di seguito riportate, di un dettaglio dei principali flussi di *reporting* attivati presso la Compagnia.

Flussi di <i>reporting</i> con le autorità esterne			
Owner	Destinatario	Frequenza	Contenuti principali
F.A. (nella persona del Responsabile della Funzione o del Responsabile SOS)	UIF	Mensile	Trasmissione dei dati aggregati previsti dall'art. 33 del D. Lgs. 231/2007 e dal provvedimento della UIF del 23 dicembre 2013
		Ad evento	- Nominativo del responsabile SOS e del referente S.A.R.A. ed eventuali variazioni dei relativi dati - Segnalazioni di operazioni sospette - Risposte tempestive ad eventuali richieste formulate - Misure applicate ai sensi del Decreto 109/2007
	IVASS	Annuale	Esiti dell'esercizio di autovalutazione del rischio di riciclaggio e finanziamento del terrorismo



Flussi di reporting con le autorità esterne			
Owner	Destinatario	Frequenza	Contenuti principali
		Ad evento	Riscontri a richieste di informazioni
	MEF	Ad evento	Comunicazioni aventi ad oggetto le misure applicate nei confronti dei clienti e delle controparti ai sensi del Regolamento CE 2580/2001 ¹¹
Collegio sindacale	MEF	Ad evento	Ai sensi dell'articolo 51, comma 1 del Decreto antiriciclaggio eventuali infrazioni alle disposizioni di cui all'articolo 49, commi 1, 5, 6, 7, 12 del Decreto stesso entro trenta giorni
	IVASS	Ad evento	Comunicazioni, ai sensi dell'articolo 46, comma 1, lettera b) del Decreto antiriciclaggio, di tutti i fatti di cui venga a conoscenza nell'esercizio delle proprie funzioni che possano costituire violazioni gravi o ripetute o sistematiche o plurime delle disposizioni di legge e delle relative disposizioni

Flussi di reporting fra le strutture aziendali			
Owner	Destinatario	Frequenza	Contenuti principali
F.A. (nella persona del Responsabile)	CdA	Almeno annuale (o in caso di significative modifiche del rischio cui l'impresa è esposta)	Relazione su: - attività svolte e verifiche compiute - valutazioni effettuate - criticità e carenze rilevate e raccomandazioni formulate per la loro rimozione, nonché sullo stato e sui tempi di implementazione degli interventi migliorativi - attività formativa - risultati dell'esercizio di autovalutazione nonché il piano delle azioni correttive ancora da intraprendere, tenuto conto delle carenze riscontrate nelle verifiche precedenti e di eventuali nuovi rischi identificati - Piano annuale delle attività antiriciclaggio e di contrasto al finanziamento del terrorismo
	Collegio Sindacale	Ad evento	Relazione su: - attività svolte e verifiche compiute - valutazioni effettuate - criticità e carenze rilevate e raccomandazioni formulate per

¹¹ Come da ultimo modificato dal Regolamento di esecuzione (UE) n. 646/2013 della Commissione, del 4 luglio 2013



Flussi di reporting fra le strutture aziendali			
Owner	Destinatario	Frequenza	Contenuti principali
			la loro rimozione, nonché sullo stato e sui tempi di implementazione degli interventi migliorativi - attività formativa
	OdV	Ad evento	Relazione su: - attività svolte e verifiche compiute - valutazioni effettuate - criticità e carenze rilevate e raccomandazioni formulate per la loro rimozione, nonché sullo stato e sui tempi di implementazione degli interventi migliorativi - attività formativa
	Amministratore Delegato Comex	Almeno Annuale	- Reporting sulla clientela PEP (analisi della clientela PEP sotto il profilo della numerosità, tipologia, caratteristiche principali) - Piano di ricertificazione della clientela ("GRP KYC")
		Almeno semestralmente	Informativa al Comitato Esecutivo (Comex) su: - attività svolte e verifiche compiute - valutazioni effettuate - criticità e carenze rilevate e raccomandazioni formulate per la loro rimozione, nonché sullo stato e sui tempi di implementazione degli interventi migliorativi - attività formativa
		Ad evento	- Criticità evidenziate dalla F.A. - Compliance Risk Assessment (es, "Top Compliance Risks")
F.A. (nella persona del Delegato SOS)	Responsabile della struttura coinvolta	Ad evento	- Con riferimento alle operazioni sospette e con modalità idonee a garantire la tutela della riservatezza anche nei confronti degli esponenti e delle altre funzioni aziendali non coinvolte nel processo di segnalazione, comunica: l'esito della propria valutazione al responsabile della unità organizzativa dell'impresa che ha effettuato la segnalazione;



Flussi di reporting fra le strutture aziendali			
Owner	Destinatario	Frequenza	Contenuti principali
			i nominativi dei clienti oggetto di segnalazione di operazioni sospette ai fini dell'attribuzione o dell'aggiornamento del profilo di rischio dei clienti stessi
Internal Audit	CdA Collegio Sindacale	Ad evento	Relazione sull'attività svolta nell'ambito della prevenzione dei rischi di riciclaggio e sui relativi esiti, fermo restando il rispetto del principio di riservatezza in materia di segnalazioni di operazioni sospette

Flussi di reporting gestionali			
Owner	Destinatario	Frequenza	Oggetto Valutazione del rischio riciclaggio e finanziamento del terrorismo e predisposizione di azioni di contrasto/ mitigazione del rischio, in riferimento ai seguenti aspetti
F.A.	Comitato Validazione Prodotti	Prima del lancio del nuovo prodotto	Validazione di un nuovo prodotto
	Comitato Accettazione/ Review Intermediari	Periodicamente	Accettazione di nuovo Intermediario Distribuito e successivo monitoraggio
	Outsourcing Committee	Ad evento	Validazione di un nuovo outsourcer
	Comitato di Sicurezza Finanziaria	Trimestrale / Ad evento	- Criticità evidenziate dalla FA/ pianificazioni interventi per risolverle - Sviluppo del business/ impatti antiriciclaggio generati - Impatti sull'operatività della Compagnia per effetto dalla modifica della normativa antiriciclaggio
	Comitato Antiriciclaggio (SOS)	Ad evento	Posizioni potenzialmente sospette di riciclaggio-terrorismo

Flussi informativi con Regulatory Controls			
Owner	Destinatario	Frequenza	Contenuti principali
Regulatory Controls	Comitato Accettazione Clienti / KYC Review	Ad evento	Accettazione e/ o revisione di un cliente ad alto rischio
		Ad evento	Dossier KYC



Flussi informativi con Regulatory Controls			
Owner	Destinatario	Frequenza	Contenuti principali
	Funzione Antiriciclaggio	Bisettimanale	Alert SOS scalati a 2° livello
		Mensile	Quality Assurance reporting su alert SOS
		Giornaliero	Report sospensive
		Ad evento	Esiti delle verifiche riguardanti le liste nominativi di sorveglianza a contrasto del finanziamento del terrorismo per successivo approfondimento di 2° livello
	Head Office	Mensile	Stato avanzamento programma ricertificazione della clientela
	BNL	Mensile	Clientela comune avente profilo di rischio disallineato ("Alto" in Cardif ed inferiore in BNL)

F.A. e Funzioni di controllo di II livello

Comunicazione conoscitiva-informativa			
Owner	Destinatario	Frequenza	Contenuti principali
F.A.	R.M.	Annuale	Contributo della F.A. alla Risk Cartography ("Risk ID")
F.A. RM	RM F.A.	Trimestrale	Contributo della F.A. al Risk Register per la parte di propria competenza e condivisione da parte di RM con la F.A. della versione finale con tutti i contributi raccolti
F.A. RM	RM F.A.	Trimestrale	Contributo e partecipazione al Comitato Rischi Operativi in cui sono portate le criticità evidenziate dalla F.A.
F.A.	R.M.	Ad evento	Confronto su metodologie di gestione del rischio

F.A. e Funzioni di controllo di III livello

Comunicazione conoscitiva-informativa			
Owner	Destinatario	Frequenza	Contenuti principali
Internal Audit	F.A.	Ad evento	Eventuali inefficienze o carenze procedurali nella gestione del rischio emerse nel corso dell'attività di verifica

3.3.1. Relazioni tra la Funzione Antiriciclaggio ed il Gruppo

Tra la Funzione Antiriciclaggio ed il Gruppo è in essere un costante flusso informativo volto a riportare sia verso Casa madre (Head Office) sia verso il Territorio le principali informazioni rilevanti ai fini di un coordinato presidio del rischio di riciclaggio.



F.A. ed Head Office

Comunicazione conoscitiva-informativa			
Owner	Destinatario	Frequenza	Contenuti principali
F.A.	Compliance Head Office	Annuale	Financial Security Yearly Risk Assessment
		Trimestrale	Key Performance Risks Indicators (indicatori quantitativi di rischio)
		Trimestrale	Compliance Risk Register
		Trimestrale	Risultati controlli "GCP" – Generic Control Plan
		Mensile	Partecipazione del Titolare della F.A. al Comitato di Management di Compliance Head Office
		Ad evento	Suspicious Activity Report (invio tramite il tool STAR)
		Semestralmente	Scambio profili di rischio alti Cardif Vita – Cardif Lux

F.A. ed il Territorio

Comunicazione conoscitiva-informativa			
Owner	Destinatario	Frequenza	Contenuti principali
F.A.	Italy Compliance Committee	Semestrale	Principali attività svolte ("key achievement"), rischi, azioni a mitigazione dei rischi e progettualità in corso
F.A.	Comitato Governance Integrata Programmi Compliance (GIPC)	Trimestrale	Principali temi di Compliance che siano di interesse comune per la Compagnia e il Partner BNL.

3.3.2. Rete distributiva diretta

L'articolo 20 del Regolamento IVASS prevede particolari presidi che le imprese devono adottare per assicurare il rispetto delle disposizioni in materia di contrasto al riciclaggio ed al finanziamento del terrorismo, nella vendita di prodotti assicurativi tramite rete distributiva diretta.

A tal fine, la Compagnia:

- ogniquale volta entra in relazione con un "nuovo Intermediario", lo sottopone ad una propria attività di verifica (due diligence), cioè ad un insieme di analisi e controlli volti a prevenire, tra gli altri, anche il rischio riciclaggio e finanziamento del terrorismo. Si rimanda per tale aspetto al capitolo VII del "Documento Analitico";
- prevede nell'ambito dei contratti/accordi di collaborazione con gli intermediari costituenti la rete distributiva diretta le regole di comportamento per prevenire il rischio di riciclaggio cui gli stessi devono attenersi nell'esercizio della propria attività, nonché la facoltà di eseguire verifiche dirette in loco;
- fornisce agli intermediari costituenti la rete distributiva diretta, gli strumenti operativi e le procedure, anche informatiche, per l'adempimento degli obblighi antiriciclaggio;



- monitora il rispetto delle regole di comportamento antiriciclaggio, ivi comprese quelle richiamate nei contratti/accordi di collaborazione;
- interviene, nei casi in cui è richiesta l'applicazione di misure rafforzate di adeguata verifica della clientela in ragione del più elevato rischio di riciclaggio, a supporto della rete distributiva diretta nell'adempimento degli obblighi di cui all'articolo 24 del Decreto antiriciclaggio.

Con i principali intermediari esistono inoltre specifici Comitati di condivisione e coordinamento delle attività di interesse comune.

F.A. e Rete Distributiva Diretta

Comunicazione conoscitiva-informativa			
Owner	Destinatario	Frequenza	Contenuto relazione
F.A.	BNL Findomestic	Almeno annuale	Condivisione tematiche di interesse comune (risultati dei controlli, necessità di sviluppo nuovi processi/presidi, condivisione avanzamento piani di azione)
BNL F.A.	F.A.	Ad evento	Clientela comune e stesse operazioni oggetto di segnalazione di operazione sospetta ex Provv. 111/2021
F.A.	F.A. BNL	Ad evento	- Clientela comune oggetto di segnalazione di operazione sospetta Request for Information (RFI) Richiesta di informazioni nell'ambito del processo di analisi degli alert relativi alle operazioni sospette

IV. STRUMENTI A SUPPORTO DELL'OPERATIVITÀ

La Funzione Antiriciclaggio si avvale di appositi strumenti informatici per svolgere compiutamente le proprie attività che sono dettagliate nei capitoli successivi. Tutti gli strumenti informatici sono collegati tra loro mediante flussi.

In particolare, si riporta una descrizione dei principali tool utilizzati.

4.1. Applicativi gestionali e tool post-vendita

Ai fini delle analisi antiriciclaggio assumono rilevanza, in prima battuta, i sistemi gestionali della Compagnia dove sono ospitati i dati della clientela e le informazioni riguardanti le operazioni da questa richieste ed eseguite.

NAIS

Sistema di gestione del portafoglio Vita (prodotti Saving, TCM). Il sistema gestisce il ciclo di vita della polizza dall'assunzione alla liquidazione.

FOREMAST

Sistema di gestione del portafoglio Vita (Protection) che gestisce tutto il ciclo di vita della polizza dall'assunzione alla liquidazione.

SMARTHALL

sistema di gestione del portafoglio Vita (Saving in *run off*, prodotti previdenziali BNL) che gestisce tutto il ciclo di vita della polizza dall'assunzione alla liquidazione;

GIPSY CLAIMS sistema di gestione dei sinistri Protection;

TOOL PLUS



applicativo di *workflow* documentale che, integrato al sistema di portafoglio Sinistri Gipsy, consente la gestione ed il monitoraggio del processo sinistri dalla ricezione della denuncia fino alla decisione di liquidazione o di rifiuto;

TOOL POST-VENDITA

front end con funzionalità di repository documentale e di workflow integrato con Gipsy claims e Foremast ed utilizzato per tracciare le operazioni e le pratiche post-vendita (dossier dematerializzati, audit trail lavorazione, etc.).

4.2. Applicativi di screening, scoring e conservazione dei dati AML

WINTAR

Al fine di osservare gli obblighi prescritti dal Decreto antiriciclaggio e dal Regolamento IVASS in materia di conservazione dei dati e delle informazioni utili a prevenire, individuare o accertare eventuali attività di riciclaggio o di finanziamento del terrorismo, la Compagnia fa ricorso all'Archivio Unico Informatico (AUI).

La soluzione tecnologica implementata dalla Compagnia per garantire la registrazione in AUI è incentrata sull'applicativo WINTAR che provvede a:

- acquisire, a partire da tutte le procedure informatiche che elaborano dati rilevanti ai fini antiriciclaggio, i diversi flussi informativi necessari alla valorizzazione dei dati all'interno dell'AUI;
- eseguire controlli preventivi sui dati, al fine di verificarne la correttezza e consistenza prima della registrazione all'interno dell'Archivio definitivo;

Il tool include anche il modulo denominato "Check Enterprise" (anche Diagnostico AUI) che consente di verificare la correttezza e coerenza dei dati registrati in Archivio Unico Informatico. In particolare, il modulo prevede due funzionalità: la prima ("Check") verifica la struttura ed il contenuto delle singole registrazioni presenti in AUI, mentre la seconda ("Advanced Check") individua eventuali incoerenze logiche nella sequenza di alimentazione dell'AUI stesso, analizzando nel loro complesso le registrazioni presenti in AUI.

KYC4

KYC4 è il tool utilizzato per l'assegnazione del rischio alla clientela (c.d. scoring), nonché per la rilevazione di operazioni potenzialmente sospette nel corso del rapporto continuativo. Le elaborazioni vengono svolte su tutto il portafoglio della Compagnia rientrante nel perimetro antiriciclaggio (clientela di prodotti con componente vita).

Il tool include anche il modulo denominato "Expansion" che consente di verificare – tramite l'algoritmo c.d. Trustify- l'appartenenza della clientela alle liste:

- SGR – Politici Italiani Locali che contiene i nominativi degli amministratori a livello locale per tutti i comuni, le città metropolitane, le province e le regioni dello Stato italiano;
- la Lista Diretta locale contenente i soggetti per i quali sono state ricevute richieste di accertamento da parte di Organi di controllo/Autorità Giudiziarie, Polizia Fiscale, allo scopo di combattere frodi, evasioni fiscali o altri comportamenti illeciti.

SUN

Il tool SUN è l'applicativo di Gruppo utilizzato dalla Compagnia per eseguire il controllo costante di presenza (c.d. ongoing screening) della clientela e delle controparti (i) nelle "liste di sorveglianza" applicabili nonché (ii) nelle liste PEP (Persone Politicamente Esposte). Le attività di screening sono effettuate in automatico incrociando i dati presenti sui sistemi della Compagnia con i nominativi oggetto di ricerca.

Le liste gestite dal Gruppo BNP Paribas sono ospitate nel database denominato REGLISS e classificate come segue:

- categoria Sanzioni, AML / CFT, Non-financial security;
- tipo Regulatory, Derivatives, Internal Policy.

Con riferimento alla categoria.

- **Sanzioni:** le liste relative ai regimi / programmi di sanzioni finanziarie sono utilizzate dai governi nazionali e dalle organizzazioni multinazionali, come le Nazioni Unite, per limitare e scoraggiare le minacce percepite alla loro sicurezza o per conformarsi alle norme internazionali riconosciute. Tali liste consentono l'individuazione e la prevenzione di transazioni finanziarie e commerciali vietate, comprese le esportazioni vietate verso / da determinati Paesi.

- **AML/CFT:** tra le liste di questa categoria rientrano tipicamente le liste PEP. In generale, esse consentono l'individuazione di clienti e la prevenzione di potenziali operazioni da sottoporre a misure rafforzate di adeguata verifica.
- **Non-financial security:** si tratta di liste escluse dal campo di applicazione della sicurezza finanziaria (ad esempio: CSR o liste di Gruppo per contrastare le frodi).

Con riferimento al tipo.

- **Regulatory:** liste ufficialmente pubblicate dalle autorità competenti (FR, UE, ONU, USA / OFAC e altre autorità di regolamentazione) che includono, a titolo esemplificativo, individui, entità, navi, aeromobili, merci, titoli (strumenti finanziari) e Paesi. Le liste regolamentari messe a disposizione dal Gruppo BNP Paribas garantiscono, quindi, il requisito normativo italiano il quale richiede la verifica delle liste definite dall'Unione Europea, dalle Nazioni Unite e dall'OFAC.
- **Derivatives:** liste interne definite sulla base di criteri e / o divieti definiti dalle autorità competenti che però non trovano ufficializzazione in liste regolamentari. Sebbene tali liste non siano emesse dalle autorità ufficiali, sono considerate "derivatives" in quanto rafforzano il presidio di conformità al requisito regolamentare riguardante:
 - o persone oggetto di sanzioni;
 - o Paesi oggetto di embarghi;
 - o ISIN oggetto di sanzioni settoriali;
 - o PEPs.
- **Internal policy:** liste interne definite dal Gruppo per integrare e rafforzare i requisiti normativi e / o per scopi di sorveglianza. Tali liste sono formate e mantenute internamente da GFS o da entità BNPP locali secondo le rispettive normative interne al fine di promuovere una conformità che sia trasversale e omogenea. I relativi contenuti non sono necessariamente obiettivi di Sanzioni ma possono rappresentare un elevato livello di rischio per il Gruppo in termini di compliance e sicurezza finanziaria.

VIGILANCE

Il tool VIGILANCE è l'applicativo di Gruppo utilizzato dalla Compagnia per eseguire il controllo puntuale di presenza (c.d. one-off screening) della clientela e delle controparti (i) nelle "liste di sorveglianza" applicabili nonché (ii) nelle liste PEP (Persone Politicamente Esposte). In particolare, oltre all'utilizzo in modalità manuale in occasione dell'adeguata verifica rafforzata della clientela, il tool viene utilizzato anche in modalità automatica in fase di pagamento dei beneficiari di prodotti di protezione (mentre lo screening in fase di pagamento dei beneficiari di prodotti risparmio rimane comunque garantito da SUN).

SGR Compliance Control: interfaccia che consente l'interrogazione delle liste:

- SGR Adverse Media Italy¹² (Liste Antiriciclaggio Italia Nominativi e Società) che contiene quasi un milione di anagrafiche di persone fisiche e giuridiche coinvolte in Italia in reati di natura penale a monte del riciclaggio. Tali reati sono riconducibili alle categorie: reati contro il patrimonio, reati contro la persona, organizzazione criminale, corruzione e tangenti, truffa e frodi, bancarotta e droga;
- SGR – Politici Italiani Locali che contiene i nominativi degli amministratori a livello locale per tutti i comuni, le città metropolitane, le province e le regioni dello Stato italiano.

¹² Alla data in cui si scrive sono in corso le valutazioni riguardanti l'opportunità di introdurre per la ricerca di notizie cc.dd. *crime* il tool di Gruppo DJAAMS e, eventualmente, la dismissione di SGR Adverse Media Italy.



V. MAPPATURA DEI RISCHI

5.1. Individuazione del rischio

La Funzione Antiriciclaggio può identificare un rischio di non conformità, reale o potenziale, in occasione, tra le altre, della conduzione delle seguenti attività:

- verifica circa il rispetto a livello aziendale dei dettami normativi (esterni ed interni), anche attraverso le attività di controllo svolte;
- esecuzione dei risk assessment periodici, di Gruppo e locali (cfr. il capitolo VI “analisi e valutazione del rischio di riciclaggio e finanziamento del terrorismo” per maggiori dettagli) funzionali ad identificare eventuali aree di miglioramento;
- partecipazione ai progetti aziendali aventi natura regolamentare, in linea con il perimetro di competenza della stessa definito nella Politica di Conformità;
- analisi degli incidenti operativi per la determinazione di quelli c.d. “Compliance related”;
- monitoraggio delle raccomandazioni formulate da parte della Funzione Antiriciclaggio e, laddove identificate, delle raccomandazioni “Compliance related”;
- partecipazione ai comitati di propria competenza e ai comitati aziendali di interesse.

5.2. Alimentazione del Risk Register

A fronte delle attività descritte al paragrafo precedente, la Funzione Antiriciclaggio procede alla determinazione della probabilità di accadimento del rischio e del relativo impatto (la cui combinazione determina il livello di rischio inerente), in linea con le metriche di valutazione definite a livello locale da parte della Funzione Risk Management come di seguito illustrate:

LIKELIHOOD							
Likely	More than one chance out of 2 that the risk occurs in the year The risk occurs at least once every 2 years					L = low risk, managed by routine procedures	Impact on the achievement of the objective is not of any concern, or is marginal- this risk is well controlled.
Very likely occurrence over 1 year (>50%)							
Possible	Between one chance out of 10 and one chance out of 2 that the risk occurs in the year The risk occurs on average once every 2 to 10 years.					M = moderate risk, management responsibility must be specified	Impact on the achievement of the objective is limited. Actions need to be undertaken but are not urgent at this stage
Possible occurrence over one year (10 to 50%)							
Rare	The risk is between 1 and 10% chance of occurring in the year. The risk occurs on average once every 10 to 100 years.					S = significant risk, senior management attention needed	Impact on the achievement of the objective is significant. We are forced to take immediate actions to mitigate the risk. Presentation in ICC
Possible occurrence over one year, but not likely (1 to 10%)							
Unlikely	Less than one in 100 chance to see the risk occurs in the year					H = high risk, immediate action needed	Impact on the achievement of the objective is of such a magnitude that the objective is highly unlikely to be met. We are forced to take immediate actions to mitigate the risk.
Unlikely occurrence over one year (<1%)							
		Qualitative	Minor	Significant	Major	Critical	
		SEVERITY					

In particolare:

- per quanto concerne la probabilità di accadimento, la stessa viene determinata principalmente sulla base dell’*expert judgement* della Funzione Antiriciclaggio, tenendo conto, laddove disponibili, dei dati di riferimento;
- per quanto attiene l’impatto del rischio, lo stesso è anch’esso stimato sulla base di un *expert judgement* della Funzione Antiriciclaggio che tiene in considerazione la possibile sanzione da parte del Regolatore e/o l’eventuale impatto reputazionale per la Compagnia.

Contestualmente, procede alla raccolta presso le funzioni aziendali interessate delle informazioni necessarie (es. procedure, controlli, adozione di azioni di *contingency*, etc), ad integrazione delle informazioni in proprio possesso, per la valutazione dell’ambiente di controllo in essere.



La valutazione dell'ambiente di controllo, opportunamente rapportato con il rischio inerente stimato, contribuirà alla determinazione del rischio residuo (*low, medium, high, very high*). In caso di rischio residuo "high" o "very high", deve essere sempre definito un apposito piano di rimedio per la relativa mitigazione che includa anche *owner* e *due date* (mutualizzazione dell'eventuale piano definito dalla prima linea di difesa, integrato, se del caso, con ulteriori azioni concordate con la Funzione Antiriciclaggio). Dopo la prima rilevazione, le azioni via via messe a terra entreranno a far parte dell'ambiente di controllo, mitigando il rischio.

Trimestralmente, la Funzione Compliance, inclusa dunque la Funzione Antiriciclaggio, viene ingaggiata da parte della Funzione Risk Management per fornire gli opportuni aggiornamenti dei rischi mappati nell'ambito del Risk Register. In taluni casi, qualora ritenuto opportuno, per i rischi comuni ad altre funzioni aziendali, la Funzione Antiriciclaggio si allinea con la prima linea di difesa sul livello di rischio da assegnare.

VI. ANALISI E VALUTAZIONE DEL RISCHIO DI RICICLAGGIO E FINANZIAMENTO DEL TERRORISMO

6.1. Autovalutazione IVASS

La Funzione Antiriciclaggio, conformemente a quanto disposto dall'articolo 14 del Regolamento IVASS, dirige e coordina l'esercizio annuale di autovalutazione del rischio di riciclaggio e finanziamento del terrorismo ("autovalutazione") cui le imprese ramo vita italiane sono esposte.

I risultati dell'esercizio ed il piano delle azioni correttive da intraprendere (inclusa la verifica dello stato di attuazione delle iniziative assunte in precedenza) sono riportati nella relazione annuale della Funzione Antiriciclaggio approvata dal Consiglio di Amministrazione.

Per lo svolgimento dell'esercizio di autovalutazione, Cardif Vita si avvale di un tool metodologico che, in modalità coerente con i principi e le policies della Compagnia, prevede:

- la possibilità di articolare le analisi per l'intera "linea di business" (i.e. polizze individuali, polizze collettive), e per "tipologia di prodotto" (i.e. prodotti di puro rischio, prodotti di non di puro rischio a vita intera, prodotti non di puro rischio a scadenza). Tale articolazione assume rilievo sia per la determinazione del rischio intrinseco, sia per l'analisi del grado di vulnerabilità dei controlli e del rischio residuo. La decisione di avallare tale articolazione è stata assunta con l'obiettivo di avere un maggior numero di informazioni di dettaglio circa il livello di esposizione al rischio della Compagnia;
- la presenza di fattori di rischio da utilizzare per la determinazione del rischio intrinseco. I fattori di rischio sono raggruppati per omogeneità sulla base dei driver forniti da IVASS (i.e. clienti, transazioni, canali distributivi) e sono valutati attraverso l'analisi della frequenza di accadimento e il relativo impatto (reputazionale e sanzionatorio);
- l'adozione di un questionario per la valutazione dei controlli necessari per la mitigazione del rischio. I controlli sono determinati sulla base di quanto previsto dalle disposizioni normative vigenti, nonché sulla base di best practices di mercato. In tale sezione del tool è, pertanto, possibile assegnare un giudizio ad ogni singolo controllo previsto, nonché descrivere i *gap* identificati e le eventuali azioni di miglioramento;
- l'impostazione di formule automatiche, che, sulla base della valutazione attribuita a ciascun fattore di rischio e del giudizio assegnato ai controlli, consentono di determinare il rischio residuo da attribuire alle singole linee di business.

Il tool offre, infine, la possibilità di avere diverse viste sui risultati delle valutazioni. Nello specifico, attraverso una serie di "drill down" è possibile ottenere, partendo dai risultati di sintesi, informazioni di maggior dettaglio circa: rischiosità dell'impresa; rischiosità della linea di business; rischiosità alla tipologia di prodotto; valorizzazione attribuita ai diversi driver e fattori di rischio.

L'esercizio di autovalutazione del rischio si articola nelle seguenti quattro fasi operative, descritte nei successivi paragrafi:

- impostazioni dell'analisi;
- analisi e valutazione dei rischi e dei controlli;
- predisposizione della relazione di autovalutazione e del remedation plan;
- compilazione prospetto IVASS.

6.1.1. Impostazione dell'analisi

Per lo svolgimento dell'esercizio di autovalutazione del rischio di riciclaggio e di finanziamento del terrorismo, la Compagnia procede a consolidare:

- l'articolazione delle famiglie di prodotto in base alla quale strutturare l'analisi del rischio e dei controlli;
- i driver di analisi da considerare (e.g. clienti, transazioni, canali distributivi) e dei correlati fattori di rischio da valutare, nonché delle metriche da utilizzare per la valutazione del livello finale di esposizione al rischio di riciclaggio finanziamento del terrorismo;
- per ciascun fattore di rischio, le informazioni necessarie per giungere alla valutazione finale del rischio inerente e la richiesta verso la struttura dell'impresa che sarà responsabile della produzione dei dati.

A tal fine, costituisce punto di partenza l'impostazione definita durante l'ultimo esercizio di autovalutazione eseguito.

6.1.2. Analisi e valutazione dei rischi e dei controlli

L'attività di analisi e valutazione dei rischi ha lo scopo di determinare l'esposizione al rischio residuo di riciclaggio e finanziamento del terrorismo. A tal fine si provvede a:

- determinare il livello di esposizione al rischio intrinseco;
- valutare il livello di vulnerabilità dei controlli, intesi come misure organizzative (anche informatiche) e controlli previsti a fronte di ciascun fattore di rischio;
- determinare il livello di rischio residuo.

Determinazione del rischio intrinseco

Il rischio intrinseco della Compagnia è riconducibile ad una delle quattro categorie di rischio di seguito indicate, così come suggerito da IVASS per una adeguata estensione dei rischi e approfondimento degli stessi:

- Basso
- Medio-basso
- Medio-alto
- Alto

Il rischio viene determinato sulla base del valore assunto da una serie di fattori di rischio rilevanti per la Compagnia (cui è associato un peso diverso in relazione al grado di rilevanza attribuito) individuati sulla base di quanto richiesto da IVASS nonché individuati da fonti internazionali (i.e. pubblicazioni FAFT e Parere Congiunto ESAs (per cui si intendono le 3 Autorità di vigilanza europee: ESMA, EBA ed EIOPA) – fattori di rischio EIOPA).

Tali fattori sono riconducibili ai seguenti driver di analisi¹³:

- Clienti
- Transazioni
- Canali distributivi¹⁴

Per ciascun fattore di rischio è calcolato un rating sulla base della combinazione di:

- frequenza, determinata come incidenza media ponderata dalla numerosità associata a ciascun fattore di rischio considerato (e.g. numero di PEP, numero di clienti segnalati, numero di liquidazioni a favore di PEP, etc.) rispetto al numero totale dell'impresa;
- impatto, determinato come incidenza media ponderata degli importi (i.e. riserve totali, premi incassati, prestazioni liquidate) associati a ciascun fattore di rischio considerato, rispetto al totale dell'impresa.

¹³ Ai fini della determinazione del rischio residuo, i fattori individuati prendono in considerazione anche quelli previsti dal Risk Mapping, illustrato al Capitolo V "Mappatura dei Rischi".

¹⁴ Si rimanda, per il dettaglio dei fattori di rischio cui ricorre Cardif Vita all'ultima relazione riepilogativa degli esiti dell'esercizio di autovalutazione approvata dal Consiglio di Amministrazione "Relazione Autovalutazione del rischio di riciclaggio e finanziamento del terrorismo".

Si riporta di seguito uno schema rappresentativo della metodologia di valutazione adottata che ha la finalità di assicurare una adeguata assegnazione finale del rischio che, soprattutto, sia la risultante non di una “automatica attribuzione” bensì di una ponderata valutazione dei rischi (soprattutto di quelli potenzialmente “medio-alti” o “alti”) per addivenire ad una determinazione finale che sia la risultante di un percorso logico e di motivazioni il più possibile oggettive e ricostruibili ex post.

		IMPATTO				
		Basso	Medio-Basso	Medio	Medio-Alto	Alto
FREQUENZA	Basso	Basso				
	Medio-Basso		Basso			
	Medio			Medio-Basso		
	Medio-Alto				Medio-Alto	
	Alto					Alto

Una volta individuato il giudizio quali-quantitativo di ciascun fattore di rischio, si procede con il calcolo del rischio intrinseco per ciascuna delle seguenti categorie:

- drivers di analisi, tipologia di prodotto assicurativo: il rischio è determinato mediante la somma normalizzata dei punteggi attribuiti ai singoli fattori di rischio riconducibili al driver/prodotto considerato e applicando delle soglie di cut-off predeterminate (ad ogni soglia corrisponde una fascia di rischio);
- linea di business: il rischio intrinseco è calcolato mediante la media ponderata dei valori assunti dalle varie tipologie di prodotti, dove il peso è determinato dal profilo di rischio generalmente assunto dal singolo prodotto sulla base delle caratteristiche proprie dello stesso;
- impresa di assicurazioni: il rischio intrinseco è determinato prendendo il più alto dei valori assunti dalle tipologie di prodotti assicurativi sottostanti, evitando così di applicare una media (semplice o ponderata) che potrebbe comportare un abbattimento fittizio (e, quindi, non reale) del livello massimo di rischio a cui risulta esposta l’impresa.

Valutazione del grado di vulnerabilità dei controlli

La valutazione del grado di vulnerabilità dei controlli, intesi come presidi organizzativi (anche informatici) e controlli previsti a fronte di ciascun fattore di rischio identificato, dipende dalla qualità di questi ultimi.

A tal fine, è necessario determinare il livello di efficacia dei presidi adottati. La valutazione del grado di efficacia delle misure organizzative e/o controlli è basata sull’idoneità degli stessi a ridurre, almeno potenzialmente, il grado di esposizione al rischio e, allo stesso tempo, a consentire il rispetto delle disposizioni normative applicabili. Tale valutazione deve tener conto, quindi, dell’esistenza o meno di un presidio, nonché della sua corretta formalizzazione, implementazione e funzionamento.

Per lo svolgimento di tale analisi si ricorre ad una check list, riconducibile alle seguenti aree tematiche:

- governo societario: ruoli e responsabilità di organi e funzioni aziendali, architettura del sistema di controlli interni, presenza di politiche di governo dei rischi;
- presidi organizzativi antiriciclaggio: nomina e definizione dei compiti dei soggetti indicati dalla normativa in tema antiriciclaggio e per il contrasto al finanziamento del terrorismo, esternalizzazione della funzione antiriciclaggio/attività antiriciclaggio. Insieme dei presidi in materia di rete distributiva;
- adeguata verifica della clientela: esecuzione delle attività di identificazione, verifica, acquisizione di scopo e natura, controllo costante e calcolo del profilo di rischio. Applicazione dell’adeguata verifica semplificata, adeguata verifica rafforzata e obbligo di astensione;
- segnalazione di operazioni sospette: presenza degli strumenti atti ad individuare le operazioni sospette da inviare all’UIF (SOS); presenza di un processo strutturato per l’invio delle SOS;
- conservazione dei dati e delle informazioni e invio all’UIF delle segnalazioni antiriciclaggio aggregate; presenza di controlli di diagnostica e quadratura;
- monitoraggio costante e controlli: esecuzione dei controlli di secondo livello da parte della Funzione Antiriciclaggio; di terzo livello da parte della Funzione Internal Audit; da parte del Collegio Sindacale;



- formazione: insieme degli obblighi formativi verso dipendenti e rete distributiva;
- flussi informativi: insieme delle comunicazioni, attività di reporting, segnalazioni richieste dalla normativa antiriciclaggio e per il contrasto al finanziamento del terrorismo;
- disponibilità di dati per l'autovalutazione: capacità di fornire i dati richiesti per l'autovalutazione del rischio di riciclaggio e finanziamento del terrorismo.

In tale fase, pertanto, viene assegnato un giudizio ad ogni singolo controllo previsto, nonché descritti i *gap* identificati e le eventuali azioni di miglioramento. La valutazione complessiva del grado di vulnerabilità dei controlli associati a ciascuna linea di business/impresa è determinata, infine, attraverso la media ponderata dei giudizi assegnati ai singoli presidi.

Si riporta di seguito la metrica prevista per la valutazione dei presidi organizzativi.

Valutazione	Giudizio	Descrizione	Grado di vulnerabilità
++	Adeguito	Misure organizzative e/o controlli in grado di mitigare efficacemente gli impatti del rischio con sistematicità	Vulnerabilità non significativa
+	Prevalentemente adeguato	Misure organizzative e/o controlli definiti con alcune debolezze non in grado di mitigare gli impatti del rischio con continuità ed affidabilità	Vulnerabilità poco significativa
-	Parzialmente adeguato	Misure organizzative e/o controlli caratterizzati da debolezze e carenze che non consentono di mitigare gli impatti del rischio in maniera efficace	Vulnerabilità abbastanza significativa
--	Inadeguato	Misure organizzative e/o controlli da prevedere in quanto inesistenti o totalmente inadeguati a mitigare gli impatti del rischio	Vulnerabilità molto significativa

Determinazione del rischio residuo

Il rischio residuo può assumere i seguenti valori:

- Non significativo
- Basso
- Medio
- Elevato

Per la determinazione del rischio residuo viene applicata la matrice proposta da IVASS, che presuppone la combinazione dei giudizi di rischio inerente e vulnerabilità dei controlli.

Rischio intrinseco	Alto				Elevato
	Medio-alto			Medio	
	Medio-basso		Basso		
	Basso	Non significativo			
		Non significativa	Poco significativa	Abbastanza significativa	Molto significativa
		Vulnerabilità dei controlli			

Applicando la matrice proposta da IVASS, il Tool consente di individuare il rischio residuo sia per le diverse linee di business considerate, sia per l'impresa nella sua interezza.

6.1.3. Predisposizione della relazione di autovalutazione e del remedation plan

Al termine dell'analisi, si procede con la formalizzazione dei risultati dell'esercizio di autovalutazione.

La relazione è strutturata in maniera da evidenziare i seguenti aspetti: approccio metodologico adottato (fasi operative, metriche di valutazione adottate, fattori di rischio considerati); famiglie di prodotti assicurativi e valutazioni attribuite

(inherent risk, control effectiveness, residual risk); drill down sui fattori di rischio ritenuti maggiormente rilevanti/impattanti per Cardif Vita; azioni correttive proposte e remediation plan.

6.1.4. Compilazione del prospetto IVASS

In aggiunta alle attività sopra descritte, Cardif Vita provvede alla compilazione e trasmissione all'IVASS di un file fornito dalla stessa autorità, unitamente agli esiti dell'esercizio di autovalutazione.

Tale file si compone, coerentemente con le ultime indicazioni fornite dall'Autorità, delle seguenti sezioni:

- Sezione I – Organizzazione, dedicata alla descrizione del modello organizzativo adottato;
- Sezione II – Premi lordi contabilizzati, contenente dati numerici concernenti la ripartizione dei premi lordi contabilizzati riferiti alla nuova produzione, depurati dai premi lordi riferiti ai clienti cessati nel corso dell'anno, con riferimento alla tipologia di prodotto, al profilo di rischio assegnato alla clientela, alle misure di adeguata verifica applicate ed al canale di vendita utilizzato alla ripartizione per fascia d'importo del premio. Per ogni dettaglio devono essere indicati l'ammontare totale dei premi e il corrispondente numero di polizze e di clienti;
- Sezione III – Prestazioni liquidate, contenente dati relativi alle prestazioni liquidate, al corrispondente numero di polizze e di percipienti. Inoltre, sono richiesti dettagli concernenti situazioni a maggior rischio (i.e. liquidazioni a favore di PEP, liquidazioni su conti esteri e verso beneficiari identificati a distanza);
- Sezione IV – Gestione e controllo, che raccoglie dati numerici che consentono di valutare i singoli momenti di presidio del rischio, con specifico riferimento ai controlli sull'attività di adeguata verifica, alla segnalazione delle operazioni sospette, alle altre attività di controllo e alle misure rafforzate applicate in presenza di specifici indicatori di rischio;
- Sezione V – Intermediari, contenente l'importo totale dei premi lordi contabilizzati intermediati dalle diverse tipologie di distributori fornendo separata evidenza dei premi acquisiti direttamente dall'impresa;
- Sezione VI – Esito dell'esercizio di autovalutazione svolto dall'impresa di assicurazioni, contenente la matrice proposta da IVASS per la determinazione del rischio residuo di esposizione a fenomeni di riciclaggio o finanziamento del terrorismo.

L'intero esercizio e gli esiti sono sottoposti a specifica valutazione da parte della Funzione Antiriciclaggio, al fine della verifica di coerenza e armonia con il rispetto dei principi di contenimento del rischio, così come declinati nell'ambito delle policies aziendali, nonché quale attenta disamina delle azioni di adeguamento, miglioramento o *remediation* che siano state suggerite in applicazione.

Quanto precede, in linea di continuità e raccordo con quanto previsto al Cap. 6.2. (cfr. "Group Risk Assessment").

6.2. Group Risk Assessment exercises

Cardif Vita svolge, inoltre, una serie di **esercizi di risk assessment interni avviati annualmente dal Gruppo**, funzionali a valutare il rischio a cui sono esposte le singole entità in materia di antiriciclaggio e antiterrorismo.

Tali attività sono condotte con periodicità annuale dalla Funzione Antiriciclaggio, chiedendo, ove necessario, il supporto e/o il contributo agli ulteriori Uffici aziendali competenti in considerazione dell'oggetto dei singoli quesiti.

Gli esercizi in questione consistono nei seguenti:

- **ML/TF Risk Classification**, relativo alla valutazione del **rischio inerente in materia antiriciclaggio e contrasto al finanziamento del terrorismo**. Il punteggio di rischio inerente è attribuito sulla base delle risposte conferite ai quesiti dell'esercizio, i quali sono suddivisi in 5 macro-ambiti (sezioni):
 - (i) *Geography* → Paese in cui l'entità ha istituito la propria sede legale;
 - (ii) *Products & Services* → tipologia dei prodotti realizzati e natura dei servizi prestati;
 - (iii) *Clients* → specificità del modello distributivo adottato e natura dei canali distributivi utilizzati;
 - (iv) *Transactions* → natura e modalità delle transazioni finanziarie eseguite;
 - (v) *Canali* → tipologia della rete distributiva utilizzata.

La metodologia di valutazione del **rischio inerente è costruita su 4 livelli di scoring**, assegnati sulla base del **punteggio totale attribuito alla singola entità** al completamento dell'esercizio¹⁵:

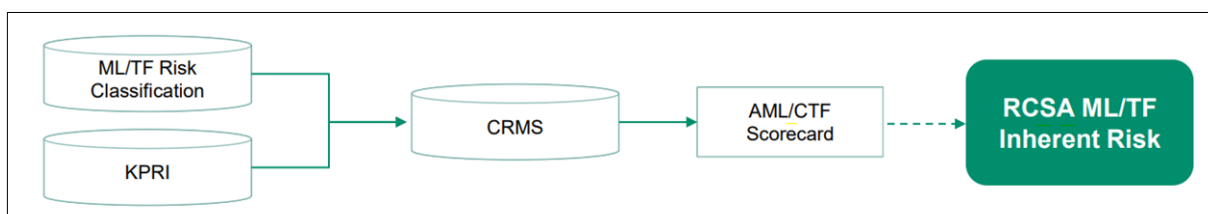
¹⁵ Il punteggio totale viene ottenuto facendo la media fra i singoli punteggi attribuiti a ciascun macro-ambito (sezione).

- *Basso*, se il punteggio totale ha valore fra 0 e 1;
- *Medio*, se il punteggio totale ha valore fra 1 e 2
- *Alto*, se il punteggio totale ha valore fra 2 e 4;
- *Molto-Alto*, se il punteggio totale ha valore fra 4 e 8.

Inherent Risk	■ Low : [0-1[	■ Medium : [1-2[	■ High : [2-4[	■ V. High : [4-8]
---------------	--	--	--	--

I risultati dell'esercizio, antecedentemente alla condivisione con il Gruppo mediante il caricamento delle risposte nel tool ufficiale denominato "CRMS" (*Compliance Risk Management System*), sono **previamente presentati all'Amministratore Delegato per certificazione**.

Inoltre, si evidenzia che una parte delle domande del ML/TF Risk Classification, congiuntamente ai KPRI di sicurezza finanziaria, sono tenute in considerazione dal Gruppo per la **determinazione del livello di rischio inerente in ambito AML/CTF** da cui la singola entità parte nell'**esercizio globale di Gruppo RCSA – Risk & Control Self Assessment**.



- *Annual Global OFAC/Sanctions Risk Assessment* (c.d. **AGORA**), volto all'esecuzione di una puntuale valutazione del **rischio residuo afferente alle sanzioni finanziari e agli 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.

È altresì svolto annualmente l'esercizio di Risk & Control Self Assessment (c.d. **RCSA**) per la valutazione dei rischi di conformità. L'esercizio è coordinato dall'Ufficio OPC nell'ambito del quale i business *owner* (1LoD) valutano i rischi individuati all'interno dei processi di cui sono responsabili, tenendo in considerazione l'efficacia dei presidi di mitigazione in essere. Tali rischi sono definiti direttamente da Head Office ed integrati localmente da parte delle Strutture responsabili. La metodologia prevede la valutazione del rischio inerente (IR) e del dispositivo di controllo (CF) e, attraverso una matrice sottostante, la determinazione del rischio residuo (RR). Tuttavia, è facoltà del business owner rivedere la valutazione di rischio residuo, modificandola e fornendo le dovute spiegazioni.

La Funzione Antiriciclaggio esegue un'attività di Check & Challenge rispetto ai rischi emersi dalle analisi delle Strutture di *Business* in tema antiriciclaggio, con la possibilità di rivedere la valutazione delle triplette effettuata preliminarmente dalla 1LoD con adeguata motivazione. Per tutte le triplette valutate con rischio residuo pari a *high* è prevista la definizione di specifici piani d'azione.

VII. DUE DILIGENCE DELLA RETE DISTRIBUTIVA

La rete distributiva intermediata attiva di Cardif Vita è attualmente composta da banche di gruppo: Banca Nazionale del Lavoro S.p.A. e Findomestic Banca S.p.A. (modello di distribuzione B to B to C), operando tali intermediari, come distributori nella commercializzazione dei prodotti della Compagnia.

Vi sono inoltre intermediari (banche o società finanziarie) in "run off", per i quali, pur essendo stato risolto l'accordo di distribuzione, rimane l'obbligo di gestione post contrattuale delle polizze, che configura l'attività distributiva ai sensi del Regolamento IVASS n. 40/2018 fino alla cessazione del contratto.

La Compagnia adotta 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 analisi preventive e nel continuo di *due diligence* che vengono aggiornate periodicamente e costituiscono condizione per il mantenimento della relazione con la Compagnia.

In particolare, è previsto:

- 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 al conseguente avvio di una nuova relazione di business con quest'ultimo, o quale condizione per confermare il mantenimento della relazione per quelle relazioni 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.

In particolare, è disposto che nei **contratti/ accordi di collaborazione** con gli intermediari costituenti la rete distributiva siano specificate le **regole di comportamento vincolanti** a fini del contrasto al riciclaggio ed al finanziamento del terrorismo cui gli stessi devono attenersi nell'esercizio della propria attività.

Negli 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 della Compagnia,

- 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.

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.

VIII. ADEGUATA VERIFICA E VALUTAZIONE DEL RISCHIO DELLA CLIENTELA

L'esecuzione delle attività di adeguata verifica è sempre disposta sia per le **polizze individuali** sia per quelle **collettive**:

- 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 venga **designato un beneficiario**, venga **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 e / o esenzione;
- qualora sorgano dubbi sulla completezza, attendibilità o veridicità delle informazioni o della documentazione acquisiti dalla clientela;
- nei confronti dei nuovi clienti, nonché dei clienti già acquisiti, quando si verifica un evento suscettibile di influenzare il livello di rischio (c.d. "trigger event" da cui scaturisce una c.d. "ricertificazione ad evento"), e, in ogni caso, secondo una frequenza predeterminata in ragione della classe di rischio assegnata (c.d. "ricertificazione periodica"), salvo eccezioni.

L'adeguata verifica della clientela consiste nelle seguenti attività:

- identificazione del cliente, dell'assicurato, del beneficiario (incluso l'eventuale percipiente)¹⁶, dell'eventuale esecutore e del terzo pagatore (ove presente), 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;
- acquisizione e valutazione di informazioni su scopo e natura del rapporto continuativo;
- esercizio di un controllo costante nel corso del rapporto continuativo.

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 implica che ai prodotti Protection, considerato il rischio intrinseco dei prodotti stessi, vengano generalmente applicate misure di adeguata verifica semplificata.

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

¹⁶ Per ulteriori dettagli si rinvia alla nota Operativa di Customer Service "Gestione della figura del terzo percipiente nel caso di Sinistri per i prodotti Saving".



dimostrare alle Autorità competenti che le specifiche misure assunte sono adeguate rispetto ai rischi rilevati nel concreto.

8.1 Acquisizione delle informazioni per i prodotti Savings

Lo strumento utilizzato per acquisire i dati identificativi della clientela e dei soggetti collegati e le informazioni sullo scopo e natura del rapporto, è la Scheda di Adeguata Verifica (**SAV**), anche definita Questionario di Due Diligence (**QDD**). Quest'ultima viene sottoposta per la compilazione nelle seguenti occasioni:

- instaurazione del rapporto continuativo;
- versamento aggiuntivo;
- cambio di contraenza;
- cambio beneficiario;
- richiesta di riscatto (totale/parziale);
- liquidazione (sinistro/scadenza)¹⁷.

In caso di apertura del rapporto viene sottoposta la Scheda di Adeguata Verifica (Nuova Emissione/Versamento Aggiuntivo). Tramite la compilazione di tale modulistica è possibile acquisire le informazioni sui seguenti soggetti:

- clienti persone fisiche, persone giuridiche e ditte individuali;
- esecutore, se diverso dal contraente, il quale è sempre previsto in caso di persona giuridica;
- assicurato, se diverso dal contraente;
- beneficiario designato;
- terzo pagatore;
- titolare effettivo sub 2), sempre previsto in caso di cliente persona giuridica;
- titolare effettivo sub 3), del beneficiario designato persona giuridica¹⁸.

In occasione del pagamento di un versamento aggiuntivo, è richiesta la compilazione del medesimo modulo acquisito in fase di emissione, ad eccezione delle informazioni relative alle figure dell'assicurato e del beneficiario designato.

Qualora il cliente richieda il pagamento di un riscatto parziale o totale, è richiesta l'acquisizione della Scheda di Adeguata Verifica – “Richiesta di Riscatto (parziale o totale) ed Adeguata Verifica”¹⁹. È previsto un modulo dedicato alle persone fisiche e un modulo dedicato alle persone giuridiche. Quest'ultimo permette la raccolta delle informazioni in riferimento ai seguenti soggetti:

- clienti;
- assicurato se diverso dal contraente;
- esecutore, se diverso dal contraente, il quale è sempre previsto in caso di cliente di persona giuridica;
- titolare effettivo sub 2). È sempre previsto in caso di cliente di persona giuridica.

Qualora il cliente richieda la liquidazione per scadenza, è richiesta l'acquisizione della Scheda di Adeguata Verifica – “Richiesta di Liquidazione per scadenza e Adeguata Verifica”. È previsto un modulo dedicato alle persone fisiche e un

¹⁷ Si specifica che Cardif non prevede l'esecuzione di operazioni di prestito.

¹⁸ Ai sensi dell'art. 2, c.1, lett. vv) del Regolamento 44/2019: “titolare effettivo”: i. 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”); ii. 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”), iii. 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 [omissis]”).

¹⁹ Si faccia riferimento alle schede di adeguata verifica presenti al seguente link <https://cyou-cardif-assurance.is.echonet/rooms/SavFormsRepository/Pagine/HomeNew.aspx>



modulo dedicato alle persone giuridiche. La compilazione può avvenire ad opera del cliente, ovvero del beneficiario qualora sia quest'ultimo a percepire la prestazione assicurativa. La SAV permette la raccolta delle informazioni in riferimento ai seguenti soggetti:

- clienti;
- assicurato, se diverso dal contraente;
- titolare effettivo sub 2). È sempre previsto in caso di cliente persona giuridica;
- beneficiario (persona fisica e persona giuridica);
- titolare effettivo sub 3) del beneficiario persona giuridica (cui si applicano le regole di cui al titolare effettivo sub 2).

In occasione dell'operazione di liquidazione per sinistro, è richiesta l'acquisizione del modulo "Richiesta di liquidazione per sinistro e adeguata verifica". È previsto un modulo dedicato alle persone fisiche e un modulo dedicato alle persone giuridiche. La compilazione avviene sempre ad opera del beneficiario. La SAV permette la raccolta delle informazioni in riferimento ai seguenti soggetti:

- beneficiario;
- titolare effettivo sub 3) del beneficiario persona giuridica;
- cliente;
- esecutore del cliente.

Con riferimento alla figura del percipiente (terzo rispetto al contraente e / o al beneficiario), si specifica che in linea generale tale figura non è ammessa. Tuttavia, è possibile consentire l'indicazione di tale figura solo in casi eccezionali (i.e. operazioni di sinistro) previa acquisizione di tutto il set informativo necessario e valutazione da parte della Funzione Antiriciclaggio nelle casistiche e nella modalità disciplinate nella nota operativa dedicata²⁰.

Qualora il cliente faccia richiesta di cambio contraenza, è necessaria l'acquisizione della Scheda di Adeguata Verifica – "Richiesta di variazione di contraenza e Adeguata Verifica". È previsto un unico modulo sia per le persone fisiche che per le persone giuridiche. La compilazione avviene ad opera del contraente uscente diverso dal caso di decesso. La SAV permette la raccolta delle informazioni in riferimento ai seguenti soggetti:

- contraente uscente, anche detto cedente, (ai fini di aggiornamento dell'adeguata verifica);
- subentrante;
- esecutore se diverso dal contraente subentrante;
- assicurato;
- titolare effettivo se contraente subentrante è persona giuridica;
- esecutore se diverso dal contraente uscente.

Infine, in occasione dell'operazione di cambio beneficiario, è richiesta l'acquisizione della Scheda di Adeguata Verifica – "Richiesta di cambio beneficiario e Adeguata Verifica".

È previsto un unico modulo sia per le persone fisiche che per le persone giuridiche. La compilazione avviene ad opera del contraente al fine di rispettare il disposto normativo che prevede che si tratti di dichiarazioni rese, per iscritto, da parte del Contraente, quindi, sottoposte a verifica di adeguatezza da parte della Compagnia.

La SAV permette la raccolta delle informazioni in riferimento ai seguenti soggetti:

- nuovi beneficiari;
- titolare effettivo del beneficiario diverso da persona fisica.

Nel caso in cui uno dei soggetti di cui sopra rivesta contemporaneamente più figure, i dati devono essere raccolti per ognuna di queste.

²⁰ Per ulteriori dettagli si rinvia alla nota Operativa di Customer Service "Gestione della figura del terzo percipiente nel caso di Sinistri per i prodotti Saving".

Al momento della compilazione della Scheda di Adeguata Verifica, vengono richieste determinate informazioni sul cliente e sui soggetti collegati, nonché sull'operazione. In particolare, in funzione dell'operazione richiesta:

- dati relativi al rapporto (e.g. canale distributivo, tipologia prodotto, importo);
- scopo e natura del rapporto continuativo (e.g. finalità del rapporto continuativo);
- tipologia di origine dei fondi (e.g. reddito da lavoro dipendente, lascito/eredità/donazione, vendita immobiliare, voluntary disclosure) e Paese di provenienza degli stessi;
- Paese di destinazione dei fondi in occasione della liquidazione della prestazione assicurativa;
- mezzi di pagamento (e.g. bonifico).

In riferimento al contraente o al beneficiario (in fase di liquidazione per scadenza o per sinistro) persona fisica, vengono raccolte le seguenti principali informazioni:

- dati anagrafici (e.g. nome, cognome, codice fiscale, cittadinanza, residenza anagrafica e, se diverso, domicilio);
- residenza fiscale;
- professione esercitata;
- status di PEP;
- dati economici del contraente (e.g. principale fonte di reddito);
- legame tra contraente e beneficiario.

In riferimento al contraente o al beneficiario (in fase di liquidazione per scadenza o per sinistro) persona giuridica vengono richieste le seguenti principali informazioni:

- dati identificativi (e.g. ragione sociale, partita iva, forma giuridica);
- sede legale della Società e luogo di costituzione;
- dati economici (e.g. fatturato annuo);
- altre informazioni (e.g. operatività/relazioni con l'estero);
- legame tra contraente e beneficiario.

Nei confronti dell'assicurato e dell'esecutore (sia esso il legale rappresentante o pagatore, nelle operazioni di incasso) vengono richiesti:

- i dati anagrafici (e.g. nome, cognome, codice fiscale, residenza anagrafica e, se diverso, domicilio);
- documenti identificativi;
- lo status di PEP;
- il legame con il contraente (ove diverso).

mentre, nei confronti dei titolari effettivi, viene richiesto di indicare:

- dati anagrafici (e.g. nome, cognome, codice fiscale, residenza anagrafica e, se diverso, domicilio);
- documenti identificativi;
- residenza fiscale;
- status di PEP;
- legame con il contraente.

8.2 Acquisizione delle informazioni per i prodotti Protection

Lo strumento utilizzato per acquisire i dati identificativi della clientela e dei soggetti collegati e le informazioni sullo scopo e natura del rapporto è la SAV in forma semplificata. A differenza di quanto accade per i prodotti Saving, dove la SAV è sempre un documento autonomo rispetto agli altri documenti contrattuali, per i prodotti Protection la scelta della Compagnia è quella di avvalersi di una SAV integrata nel modulo di adesione del prodotto stesso. Quest'ultima viene sottoposta per la compilazione:

- al momento dell'instaurazione del rapporto continuativo;

- in occasione di liquidazione per sinistro / estinzione anticipata.

Tramite la compilazione di tale modulistica vengono acquisite le informazioni sui seguenti soggetti (ove applicabili al prodotto):

- clienti persone fisiche, persone giuridiche e ditte individuali;
- esecutore, se diverso dal contraente/aderente. È sempre previsto in caso di persona giuridica;
- assicurato, se diverso dal contraente/aderente;
- beneficiario designato;
- terzo pagatore;
- titolare effettivo sub 2), sempre previsto in caso di cliente persona giuridica;
- terzo percipiente in caso di liquidazione per sinistro.

8.3 Verifica delle informazioni

L'intermediario o la Compagnia (per la gestione diretta della propria clientela), acquisisce i **dati identificativi** mediante la compilazione della modulistica descritta nei precedenti paragrafi.

I dati identificativi dei **soggetti persone fisiche** sono verificati confrontandoli con le informazioni contenute in un documento di riconoscimento ai sensi della normativa vigente (i.e. carta d'identità, passaporto, patente di guida) del quale va appurata l'autenticità e la validità.

I dati identificativi dei **soggetti persone giuridiche** (soggetti differenti da persone fisiche) possono essere anche verificati effettuando il riscontro degli stessi tramite fonti esterne affidabili ed indipendenti:

- visura camerale, atto costitutivo, statuto;
- registro italiano delle imprese;
- albi ed elenchi di soggetti autorizzati;
- bilanci o documenti equivalenti;
- comunicazioni rese al pubblico in conformità alla normativa di settore (inclusi prospetti, comunicazioni di partecipazioni rilevanti o informazioni privilegiate);
- registri dei titolari effettivi istituiti negli Stati membri conformemente alla normativa comunitaria;
- informazioni provenienti da organismi e autorità pubbliche, ivi compresa la pubblica amministrazione, anche di altri Paesi comunitari, incluse quelle che possono essere acquisite attraverso i siti web.

Con riferimento alla **titolarità effettiva**, le fonti di riscontro (incluso il registro di "titolarità effettiva") consentono di ricostruire l'assetto proprietario e di controllo del cliente/beneficiario, al fine di individuare il titolare effettivo e verificare l'attendibilità delle informazioni sullo stesso fornite dal cliente/beneficiario ovvero esecutore.

Per quanto riguarda la figura dell'**esecutore**, invece, l'attività di verifica viene eseguita 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 beneficiario²¹ (i.e. provvedimento del giudice, procure notarili, visura camerale, verbale del Consiglio di Amministrazione).

Per i soggetti minori di età, i dati identificativi devono essere verificati, in mancanza di un documento di identità o di riconoscimento, attraverso il certificato di nascita o l'eventuale provvedimento del giudice tutelare. La verifica può avvenire anche a mezzo di una foto autenticata. In tal ultimo caso, devono essere acquisiti gli estremi dell'atto di nascita dell'interessato.

Per i soggetti non comunitari, sono verificati i dati personali attraverso il passaporto, il permesso di soggiorno, il titolo di viaggio per stranieri rilasciato dalla Questura, o altro documento da considerarsi equivalente ai sensi della normativa italiana.

²¹ Si specifica che il Regolamento prevede che il premio assicurativo – ad eccezione dei versamenti aggiuntivi, che il contraente non è obbligato contrattualmente a corrispondere – può essere pagato da un soggetto diverso dal contraente, anche senza essere dotato di specifico potere rappresentativo o senza fornirne documentazione (cfr. art. 57 "Adempimento dell'obbligo di pagamento di premi assicurativi").

Permane fermo il principio e la regola operativa generale che qualora dovessero emergere dubbi sulla documentazione raccolta, dovranno essere effettuati ulteriori approfondimenti applicando il regime di “adeguata verifica rafforzata” e si provvede a valutare l’avvio del processo di segnalazione di operazione sospetta.

8.4 Determinazione del profilo di rischio della clientela

Il profilo di rischio della clientela è determinato sulla base dei dati e delle informazioni acquisite tramite i questionari di Adeguata Verifica. L’analisi della profilatura della clientela per finalità antiriciclaggio si rivolge ai clienti che sottoscrivono sia prodotti Saving che Protection con componente vita.

Il profilo di rischio è elaborato in automatico ricorrendo ad algoritmi predefiniti implementati in un apposito modulo informatico denominato “Classifier”, presente nell’applicativo “KYC” versione 4 fornito dalla società Corvallis S.p.A.. La soluzione informatica anzidetta, rappresenta un prodotto di assistenza alla profilatura ampiamente diffuso nel settore di riferimento, il cui funzionamento è sottoposto alla valutazione e al monitoraggio del Responsabile della Funzione Antiriciclaggio che mantiene, rispettivamente: (i) il diritto di chiedere ogni utile o necessaria modifica o integrazione affinché i risultati proposti siano in linea con la metodologia e la classificazione di rischio prevista e deliberata dalla Compagnia; (ii) la determinazione finale da assegnare, soprattutto, in riferimento ai Clienti per i quali si debba rendere necessaria l’applicazione di misure di adeguata verifica rafforzata.

Quanto precede consente di pervenire sempre alla puntuale valutazione di ogni dato, informazione e/o elemento e così provvedere all’assegnazione a ciascun cliente di una classe di rischio che, in linea generale, mantiene il principio di associazione ad un coerente livello di profondità ed estensione degli adempimenti di adeguata verifica.

Più puntualmente, il modello di profilatura si basa sui seguenti principali criteri:

- ogni cliente è incluso in una delle classi di rischio determinate dalla Compagnia in ragione della combinazione tra classificazione del prodotto della Compagnia, con tutti gli “eventi di rischio” rinvenibili e/o associabili anche al Cliente, sempre tenuto conto delle autonome valutazioni del Responsabile della Funzione Antiriciclaggio (i.e. sia quale implementazione di regole idonee alla classificazione per tipologia di “prodotto” sia anche temperando ogni e qualsivoglia approfondimento di rischio che si renda necessario), ed un rischio “più elevato” che possa essere assegnato al Cliente da parte di altre entità di Gruppo ovvero in dipendenza di attività di approfondimento, di analisi o anche di segnalazione che siano state effettuate dai Partner della rete distributiva.

Per ogni e miglior precisazione, si specifica che:

- a) le classi di rischio sopra rappresentate sono state determinate coerentemente con i principi e le policy di Gruppo, anche in considerazione dell’avviato processo di progressiva mutualità del profilo di rischio con le altre entità del Gruppo BNPP (i.e. recepimento della IV Direttiva UE);
 - b) a ciascuna classe di rischio è associato un coerente livello di profondità ed estensione degli adempimenti agli obblighi previsti dalla normativa di contrasto del riciclaggio e del finanziamento del terrorismo, anche in raccordo e dipendenza dei profili di rischio assegnati dal principale Distributore;
- il profilo di rischio calcolato sul cliente tiene conto, ove presenti, anche delle caratteristiche dei soggetti c.d. correlati al cliente stesso, quali: l’assicurato, il beneficiario, il titolare effettivo, l’esecutore.

Gli elementi di rischio individuati dalla Compagnia ai fini dell’attribuzione del profilo di rischio del cliente sono riconducibili alle seguenti macro-categorie:

- eventi impeditivi/restrittivi dell’operatività: esiti di eventi “impeditivi” quali l’individuazione di soggetti designati e/o oggetto di sanzioni internazionali, di soggetti che hanno commesso crimini connessi al riciclaggio e finanziamento del terrorismo;
- eventi ad “alto rischio”:
 - esiti delle verifiche circa lo status di Persona Politicamente Esposta o di persona che ricopre cariche pubbliche che aumentano l’esposizione al rischio di corruzione;
 - esiti degli “eventi di rischio specifici” in riferimento ai soggetti per i quali sono pervenute richieste di accertamento - anche patrimoniale/sequestro e/o altri provvedimenti restrittivi da parte delle autorità;
 - soggetti precedentemente oggetto di una valutazione ai fini della segnalazione alla UIF anche da parte del principale Distributore;
- altri eventi ad “alto rischio”:

- forma giuridica del cliente/beneficiario persona giuridica;
- attività economica (i.e. ATECO, professione esercitata);
- reddito e patrimonio;
- anzianità della relazione;
- rischio geografico (i.e. area di residenza ovvero di svolgimento dell'attività economica);
- comportamento intrattenuto all'atto dell'apertura del rapporto o al compimento dell'operazione;
- prodotto sottoscritto che presenta potenziali rischi²²;
- valore di riserva investito nel singolo prodotto (in caso di prodotti risparmio) e valore complessivo degli investimenti presso la Compagnia (c.d. asset under management - AuM).

Rappresenta un eventuale “parametro correttivo” al rischio determinato dal sistema di profilatura, oltre alla intercorsa segnalazione di operazione sospetta, ogni evento esterno (*trigger event*) che comporti un intervento, immediato e diretto, di analisi da parte della Compagnia che prescindendo dalla “generica classificazione di rischio” (avendo anzi effetto tempestivo e diretto sull'innalzamento dello stesso rischio), ivi inclusi i flussi informativi provenienti dalla rete distributiva concernenti posizioni/operatività ad alto rischio.

Sul punto, si sottolinea che anche la sottoposizione ad “adequata verifica”, attuata in dipendenza di operatività su rapporto, ha un effetto di rinnovazione del rischio stesso.

In ogni caso, la Funzione Antiriciclaggio mantiene sempre il diritto di procedere a determinare una variazione del profilo di rischio, tenendo opportunamente traccia delle motivazioni sottostanti, qualora ritenga che la classe di rischio assegnata dal sistema di profilatura non rappresenti correttamente l'esposizione al rischio di riciclaggio e finanziamento del terrorismo del cliente.

L'attribuzione del profilo di rischio avviene principalmente mediante il ricorso alla media ponderata con inclusione di specifici elementi deterministici per l'analisi di rischi alti.

La determinazione avviene prendendo in considerazione il peso attribuito a ciascun elemento di rischio e il punteggio associato alla relativa informazione acquisita (e.g. al paese di residenza è assegnato un punteggio diverso in base al paese indicato), entrambi individuati in base alla relativa rischiosità in termini di esposizione al rischio di riciclaggio e finanziamento del terrorismo.

Il valore così calcolato è ricompreso in un intervallo definito. A ciascun intervallo, è associato un profilo di rischio.

Livello di rischio	da	a
IRRILEVANTE	1,00	1,75
BASSO	1,76	2,40
MEDIO	2,41	3,20
ALTO	3,21	5,00

In particolare, conformemente al “risk based approach”, il modello prevede la presenza di elementi scatenanti cui sono associati dei fattori di rischio al verificarsi dei quali viene assegnato un profilo di rischio “Alto” ma con scoring pari a 5. In presenza di uno di questi elementi, il peso degli altri è influente.

I fattori scatenanti sono:

- 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);

²² Infine, in argomento, a miglior chiarificazione e al di fuori di ogni analisi di rischio individuato come imminente e/ o potenziale, si richiamano i cd. “movimenti/le operazioni post vendita” ovvero sia i flussi monetari che sono attuati sui rapporti e sono tra gli elementi considerati di rilevante importanza nella valutazione globale del livello di rischio dell'intero rapporto assicurativo.



- 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);
- 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 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.

Oltre agli elementi scatenanti, il sistema di profilatura si compone di:

- elementi “semplici”: elementi che singolarmente, ciascuno con il proprio peso, contribuiscono al livello finale di scoring tramite la media ponderata;
- elementi “esclusioni”: elementi che singolarmente, ciascuno con il proprio peso, contribuiscono al livello finale di scoring, ma che vengono alternativamente attivati a seconda delle caratteristiche del cliente analizzato (i.e. persona fisica, nazione Italia/Estero);
- elementi “correlazioni”: nati dalla combinazione/raffronto tra due elementi semplici. Ogni elemento “correlazioni” con il proprio peso contribuisce al livello finale di scoring.

Il livello di *scoring* totale, in assenza di elementi “scatenanti”, è il prodotto della sommatoria degli elementi “semplici”, “esclusioni” e “correlazioni” ognuno con il proprio valore moltiplicato per il relativo peso (media ponderata). Tale valore può assumere il valore massimo di 4,99 (essendo il valore 5, come detto sopra, riservato ai rischi alti determinati per la presenza di elementi scatenanti).

Per ciascun cliente si provvede all’assegnazione di una classe di rischio successivamente all’apertura del rapporto od operazione, nonché in via continuativa se si verifica una variazione dei dati precedentemente acquisiti o un evento tale da incidere sull’esposizione del rischio del cliente, ovvero sia accertata un’operatività sospetta.

In conclusione, il livello di rischio è calcolato automaticamente sulla base dell’algoritmo opportunamente definito dalla Funzione Antiriciclaggio anche tenuto conto, nei limiti tecnici determinati dalla soluzione informatica adottata, dei requisiti di *scoring* del Gruppo. Laddove sia ritenuto opportuno in seguito alla rilevazione di situazioni significative di rischio (e.g. accertamenti assicurativi provenienti dalle Autorità), il profilo di rischio Alto può essere inoltre determinato direttamente dalla Funzione Antiriciclaggio intervenendo sulla posizione del cliente.

Per maggiori dettagli gli elementi di rischio componenti l’algoritmo di profilatura si rimanda all’Allegato 1 - Modello di profilatura Cardif Vita.

8.4.1 Profilo di rischio acquisito da BNL

Con riferimento alla clientela intermediata dal Partner BNL, la Compagnia acquisisce, attraverso Allineamento Anagrafico, il profilo di rischio assegnato dalla banca in qualità di Primary Site, applicando così il c.d. principio di reliance stabilito dalle policy di Gruppo. Il modulo “Classifier” del tool KYC, attraverso la c.d. “profilatura di Gruppo” fa prevalere, e quindi assegna al cliente in via definitiva, il profilo più alto tra quello calcolato dal tool KYC e quello acquisito da BNL.

Per gestire i casi di profilo di rischio disallineato con BNL, in particolare Alto per la Compagnia e più basso per la banca, è previsto un processo di comunicazione mensile al partner delle posizioni interessate. Una volta ricevuto l’elenco in parola, BNL provvede a sua volta con l’innalzamento del profilo registrato nei propri sistemi.

8.1.1 Profilo di rischio acquisito da Cardif Lux



La Funzione Antiriciclaggio ha inoltre sviluppato un processo funzionale all'acquisizione dei profili alti assegnati alla clientela comune da parte di Cardif Lux. Per eseguire tale allineamento, è stato sottoscritto un accordo di servizio con BNPP Cardif GIE (Cardif Head Office) che semestralmente si occupa di eseguire un *matching* tra il portafoglio risparmio della Compagnia e i soli clienti di Cardif Lux aventi le seguenti caratteristiche:

- profilo di rischio alto;
- residenza e/o cittadinanza in Italia.

8.2 Misure semplificate di adeguata verifica

Su specifica indicazione della Funzione Antiriciclaggio, possono essere adottate delle misure di adeguata verifica semplificata al momento dell'apertura del rapporto d'affari, nel corso del rapporto e in occasione delle operazioni seguenti all'entrata in relazione, per determinate categorie di clienti, rapporti e prodotti purché:

- sussistano e siano documentabili le condizioni e caratteristiche specificamente definite dalla normativa e dalla regolamentazione attuativa;
- non siano ravvisabili elementi o rischi che ne rendano incompatibile l'attuazione.

Coerentemente con i principi disciplinati dall'articolo 23 del Decreto antiriciclaggio, la Compagnia applica 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. Permane ferma una riclassificazione nell'ambito della adeguata verifica ordinaria o rafforzata nell'ipotesi di, sopraggiunto, cambio di circostanze.

Le condizioni necessarie per consentirne 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 ordinaria o 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 BASSO²³

Le misure 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.**

²³ IRRILEVANTE nel caso di clientela Protection acquisita in data anteriore all'estensione del perimetro di adeguata verifica anche ai prodotti Protection con premio annuo inferiore a 1.000 euro ovvero premio unico inferiore a 2.500 euro.

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 a 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**.

8.3 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 esposti 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 ricertificazione, 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 dedicata²⁴, 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, del 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.

²⁴ Cfr. IT-CPL-23-IT Politica applicabile alle relazioni con Persone Politicamente Esposte (PEP).

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

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.

8.3.1 Assegnazione status PEP

L'individuazione della clientela con qualità di PEP avviene principalmente sulla base:

- delle informazioni trasmesse dai Partner (in particolare attraverso l'Allineamento Anagrafico in essere con BNL);
- degli screening condotti nel continuo attraverso l'applicativo SUN²⁵.

La qualità di PEP, rilevata in relazione al cliente o ad un soggetto ad egli correlato, determina direttamente l'assegnazione del profilo di rischio alla posizione interessata e, conseguentemente, l'applicazione di misure rafforzate di adeguata verifica.

L'entrata in relazione e il mantenimento della stessa con il soggetto PEP sono autorizzate rispettivamente in seno ai Comitati CAC e KYC Review.

Con riferimento alle attività di monitoraggio e reporting, è prevista un'informativa semestrale all'Alta Direzione e al Gruppo predisposta da Regulatory Controls e presentata dalla Funzione Antiriciclaggio in cui sono rappresentati i volumi della clientela direttamente o indirettamente avente qualifica di PEP.

8.3.2 Blocchi sospensivi

Con il termine "Blocco Sospensivo" si indicano gli eventi definiti dalla Compagnia che in fase di apertura di nuovo contratto o di movimenti di post-vendita ivi compresa la liquidazione, comportano la sospensione della regolare esecuzione dell'operazione permettendo alla Compagnia di condurre una valutazione approfondita in maniera preventiva. Il Blocco Sospensivo è automatico per le operazioni intermedie dal Partner BNL (c.d. sospensiva esterna), mentre è manuale per le operazioni gestite direttamente dalla Compagnia (c.d. sospensiva interna).

A seguito della richiesta di autorizzazione a procedere da parte del gestore di BNL o del Customer Service, il dossier riguardante il prospect o il cliente viene analizzata dall'ufficio Regulatory Controls in qualità di prima linea di difesa. In assenza di elementi di anomalia Regulatory Controls procederà con l'autorizzazione al richiedente. In caso contrario il dossier sarà inviato in valutazione alla Funzione Antiriciclaggio in qualità di seconda linea di difesa che, dopo l'espletamento degli approfondimenti necessari, potrà decidere di dare corso o meno alla richiesta pervenuta.

Rientrano in perimetro le seguenti tipologie di operazioni:

- nuova emissione;
- versamento aggiuntivo;
- richiesta di riscatto parziale;
- richiesta di riscatto totale;
- richiesta di liquidazione per scadenza;
- richiesta di liquidazione per sinistro (gestione operativa interna - solo da Customer Service);

²⁵ Le istruzioni operative fornite dalla Funzione Antiriciclaggio e in uso alla prima linea di difesa per la gestione dei Blocchi Sospensivi sono pubblicate al seguente percorso W:\Area-194\REPOSITORY UFFICIO REGULATORY CONTROLS\SCHEDE REGOLA\SUN -SANZIONI e PEP.



- variazione contraenza;
- variazione Beneficiario²⁶.

Di seguito si riporta l'elenco (a titolo esemplificativo e non esaustivo) dei blocchi sospensivi informatici²⁷:

- corrispondenze liste terroristi omonimia;
- legami con Paesi sotto embargo o ad altro rischio;
- operazioni sospette (clienti oggetto di SOS all'UIF);
- domicilio/residenza/residenza fiscale estera;
- cariche ricoperte in ambito politico e istituzionale, societario, in associazioni o fondazioni;
- professioni a rischio (persone fisiche);
- entità rientrante nel perimetro MSC (Major Sanctioned Countries, ad oggi Cuba, Iran Siria, Nord Corea, Regione Crimea/Sebastopoli);
- SAE e ATECO a rischio;
- esistenza pregiudizievoli;
- PEP/PIL;
- beneficiario PEP/PIL (Vita/Morte);
- origine dei fondi/provvista "rischiosa";
- Titolare effettivo secretato

Maggiori dettagli riguardanti i Blocchi Sospensivi attivi per le operazioni intermedie da BNL sono contenuti nell'Allegato 2 - Eventi sospensivi.

Le istruzioni operative fornite dalla Funzione Antiriciclaggio e in uso alla prima linea di difesa per la gestione dei Blocchi Sospensivi sono pubblicate al seguente percorso W:\Area-194\REPOSITORY UFFICIO REGULATORY CONTROLS\SCHEDA REGOLA\SCHEDA REGOLA SOSPENSIVE.

8.3.3 Acquisizione da parte delle Società Fiduciarie dell'attestazione di adeguata verifica

Una volta che la Società fiduciaria ha assolto gli obblighi di adeguata verifica nei confronti del fiduciante e dell'effettivo beneficiario in conformità con quanto disposto dal Decreto antiriciclaggio e sempre previa verifica e conferma dell'avvenuto accertamento della congruità dei capitali oggetto di conferimento e dell'origine lecita dei fondi, il processo nei confronti della Compagnia, avviene secondo modalità prestabilite:

- acquisizione da parte di Cardif Vita nei propri sistemi di portafoglio del flusso avvenuto tramite Bancassurance da parte di BNL;
- individuazione della posizione in AUI da parte dell'Ufficio Regulatory Controls attraverso un blocco informatico impostato sulle società fiduciarie;
- inoltra della richiesta di integrazione alla Funzione Antiriciclaggio la quale predispone la richiesta di compilazione dell'attestazione di avvenuta adeguata verifica del fiduciante, nonché all'effettivo Beneficiario (nel caso in cui la fiduciaria sia il beneficiario formale), trasmettendola alla Fiduciaria;
- la Fiduciaria provvede a compilare l'attestazione di identificazione e di adeguata verifica e a ritrasmetterla alla Funzione Antiriciclaggio della Compagnia;
- una volta ricevuta la documentazione le informazioni relative al fiduciante vengono registrate in Archivio Unico Informatico.

²⁶ La Compagnia ha provveduto all'approvazione di un apposito Manuale "IT -REGC-03-IT Gestione degli eventi Sospensivi" cui si rimanda per ulteriori approfondimenti.

²⁷ Per la lista completa dei blocchi sospensivi si rimanda all'Allegato 2 – Eventi sospensivi.

8.4 Ricertificazione del cliente

Cardif Vita prevede l'aggiornamento della adeguata verifica e del conseguente profilo del rischio del cliente (cosiddetta "ricertificazione nel continuo della conoscenza del cliente"²⁸) 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), quali ad esempio:
 - l'innalzamento del livello di rischio in alto, anche da parte del tool di profilatura;
 - il rifiuto o il blocco di un'operazione;
 - la segnalazione di un'operazione sospetta;
 - notizie pregiudizievoli/procedimenti penali;
 - accertamenti svolti dalle Autorità di controllo;
 - un cambio di circostanza (i.e. trasferimento della residenza in un Paese ad alto rischio).

8.4.1 Ricertificazione periodica

La ricertificazione periodica è prevista sistematicamente in relazione alla clientela Saving con profilo Alto. La Funzione Antiriciclaggio può decidere tuttavia di inserire nel piano di ricertificazioni programmate (c.d. Global Recertification Plan – GRP) anche clientela Protection che presenti particolari elementi di anomalia.

In particolare, con riferimento alla clientela intermediata da BNL, l'applicazione del c.d. principio di "reliance" previsto dalle policy di Gruppo (cfr. CPL0252 KNOW YOUR CLIENT Global Policy) garantisce alla Compagnia (in qualità di "Secondary Site" come da definizione concordata e applicata all'interno del Gruppo) di beneficiare delle attività di ricertificazione condotte dal Primary Site (BNL), acquisendo automaticamente i dati aggiornati attraverso l'Allineamento Anagrafico.

Più in particolare il Primary Site:

- è responsabile della raccolta di informazioni e della documentazione fornite dal cliente;
- è, inoltre, responsabile della raccolta della documentazione da fonti interne o pubbliche, dell'eventuale ricerca di informazioni sfavorevoli e della valutazione del rischio cliente, secondo gli standard del Gruppo.

Con riferimento invece alla clientela non intermediata, la Compagnia verifica la presenza nei sistemi gestionali di dati eventualmente raccolti non oltre i 12 mesi precedenti (ad esempio in occasione di un'operazione postvendita) sulla base dei quali rinnovare la valutazione della relazione. In assenza, contatta direttamente il cliente richiedendo la compilazione di una nuova SAV.

Nel caso di impossibilità a completare il processo di ricertificazione (e.g. mancata risposta da parte del cliente), la Compagnia prevede fino a 2 comunicazioni di sollecito e quindi l'apposizione di un blocco operativo per impedire qualsiasi azione dispositiva in assenza di preventiva valutazione della Funzione Antiriciclaggio.

I clienti che all'esito della ricertificazione registrano un innalzamento del rischio in Alto sono portati all'attenzione dei competenti comitati interni per le opportune determinazioni (si veda anche il capitolo IX).

8.4.2 Ricertificazione ad evento

Nei casi in cui per un cliente non sia già calendarizzata la ricertificazione, la stessa potrà avvenire, con le medesime regole descritte nel paragrafo precedente, laddove siano rilevanti cambiamenti di circostanze e / o elementi significativi suscettibili di modificare il profilo di rischio (e.g. assegnazione profilo Alto nel tool KYC, Blocco sospensivo).

²⁸ Per maggiori approfondimenti si veda la Policy "Know Your Customer General Policy BNP Paribas Cardif".

IX. PROCESSI DECISIONALI E COMITATI

I processi decisionali inerenti alle tematiche antiriciclaggio prevedono il coinvolgimento della Funzione Antiriciclaggio e/o del suo Responsabile, nonché la partecipazione di tutti gli uffici aziendali che contribuiscono direttamente e indirettamente ad agire i presidi antiriciclaggio stabiliti dalla Compagnia. Tali processi decisionali sono attuati principalmente in seno:

- al Comitato Accettazione Clienti ("CAC") al Comitato KYC Review;
- al Comitato Antiriciclaggio (cui partecipa il Delegato SOS);
- al Comitato di Sicurezza Finanziaria (interno e coi Partner BNL e Findomestic).

9.1. Comitati CAC e KYC Review

I Comitati CAC e KYC Review hanno lo scopo di assumere collegialmente le decisioni riguardanti, rispettivamente, l'entrata in relazione con la clientela e il mantenimento della stessa relazione.

Sono convocati dal Segretario (membro dell'Ufficio Regulatory Controls) tramite mail inviata ai partecipanti unitamente ai dossier oggetto di adeguata verifica rafforzata e caratterizzati da un profilo di rischio alto e/o dalla presenza di anomalie meritevoli dell'attenzione dei membri dei comitati stessi.

I membri permanenti sono:

- il Responsabile della Compagnia, ciò a dire l'Amministratore delegato o il Co-manager o delegati;
- il Responsabile Direzione commerciale (con il ruolo di RM) o delegato;
- il Responsabile della Funzione Antiriciclaggio o delegato responsabile della Sicurezza Finanziaria, accompagnato dal Compliance Officer incaricato della revisione del dossier se diverso.

I membri permanenti possono invitare altri partecipanti.

Per maggiori dettagli sul processo si rimanda ai documenti Accettazione Clienti (CAC) Policy – IT-CPL-30-IT e IT-OPS-09-IT Due Diligence Clientela Esterna/Interna Dossier clientela diretta e indiretta, ricertificazioni e Soggetti PEP/ sensitive PEP/PIL e RCA.

9.2. Comitato Antiriciclaggio

Il Comitato Antiriciclaggio è composto dai seguenti membri:

- Delegato SOS nonché Responsabile della Funzione Antiriciclaggio;
- Responsabile dell'Ufficio Financial Security;
- Analista della Funzione Antiriciclaggio che ha svolto le verifiche sulle posizioni oggetto di decisione.

Il Comitato esamina attentamente i documenti che costituiscono il dossier della relazione oggetto di analisi e propone al Delegato SOS le possibili azioni da intraprendere.

A seguito dell'analisi effettuata congiuntamente, il Delegato SOS decide se procedere a:

- archiviare la posizione;
- segnalare all'U.I.F. il cliente (a valere su tutti i relativi rapporti e con ogni informazione utile sia in ordine ai legami - ad es. titolare effettivo - sia al dettaglio informativo e alle operazioni anomale, con la relativa documentazione ove di utilità alla segnalazione) e attuare ogni misura connessa, idonea e coerente, con il "rischio segnalato";
- richiedere la sospensione (ex art. 6 co. 4 D. Lgs. cit.) all'U.I.F.;
- richiedere l'inserimento del blocco operativo (c.d. *freeze*) sul nominativo;
- procedere ad informare le altre Società del Gruppo Assicurativo e/o del Gruppo BNPP, contattando le relative Funzioni Antiriciclaggio affinché, ferma la riservatezza delle informazioni e l'autonomia delle decisioni, possano essere adottate misure omogenee e conformi al rischio Antiriciclaggio.

L'analista della Funzione Antiriciclaggio redige il verbale della riunione del Comitato e provvede, dopo la raccolta delle firme di tutti i partecipanti, alla sua archiviazione.



9.3. Comitato Sicurezza Finanziaria

Il Comitato ha principalmente lo scopo di:

- 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;
- analizzare i risultati delle attività di controllo di I e di II livello condotte in ambito Financial Security con riferimento a tutte le tematiche (Antiriciclaggio - Antiterrorismo, Sanzioni finanziarie ed Embarghi), nonché qualora siano state rilevate anomalie, condividere le raccomandazioni formulate per la loro rimozione;
- monitorare lo stato e i tempi di implementazione degli interventi correttivi in corso;
- analizzare il piano delle azioni correttive ancora da intraprendere, tenuto conto delle carenze riscontrate nelle verifiche precedenti e di eventuali nuovi rischi identificati;
- supervisionare nel tempo le attività aziendali poste in essere per la conformità alle disposizioni previste dalle normative fiscali internazionali (es. FATCA ed AEOI, DAC6), fornendo supporto sulle questioni di rilevanza e su tutte quelle tematiche che superano l'ordinaria gestione degli adempimenti previsti dalla relativa normativa di riferimento, fornendo indicazioni di indirizzo strategico e valutando, quando necessario, le azioni da intraprendere per quanto concerne la corretta risoluzione delle criticità e/o delle problematiche.

I membri permanenti sono:

- il Responsabile Antiriciclaggio (che svolge il ruolo di Presidente);
- il Responsabile ETO (COO) o un suo delegato;
- il Responsabile Customer Service o un suo delegato;
- il Responsabile Operations Controls o un suo delegato;
- il Coordinatore dell'Ufficio Financial Security;
- i Coordinatori dei team KYC & Alert management e Control & Reporting.

Con le medesime finalità del Comitato di Sicurezza Finanziaria interno si svolgono, almeno una volta l'anno e comunque laddove sia ritenuto necessario, i Comitati di Sicurezza Finanziaria con i Partner infragruppo BNL e Findomestic.

X. TRANSACTION MONITORING

Cardif Vita svolge nel corso del rapporto continuativo un controllo costante dell'operatività posta in essere dalla clientela, volto ad individuare elementi di incongruenza che possano costituire anomalie rilevanti da cui potrebbero scaturire segnalazioni di operazioni sospette²⁹.

A tal fine, la Compagnia ricorre al sistema di transaction monitoring fornito dall'outsourcer Corvallis S.p.A. (Modulo "Control" dell'applicativo "Suite KYC") il quale, al verificarsi di un'operatività realizzata dal cliente da considerarsi potenzialmente anomala, genera appositi *alert* (c.d. "*alert AML*") in seguito analizzati dalla struttura di middle office (Ufficio Regulatory Controls), deputata a svolgere i controlli e le analisi di primo livello in materia antiriciclaggio, antiterrorismo ed embarghi finanziari nonché gestire la fase istruttoria ed, in caso di sospetto, determinare l'attivazione dell'iter di escalation alla funzione di secondo livello³⁰.

L'individuazione dell'operatività potenzialmente anomala, e pertanto la generazione degli alert, si basa su una serie di indicatori di anomalia definiti prendendo in considerazione le seguenti fonti normative:

²⁹ Si precisa che il transaction monitoring è una delle attività che consente il monitoraggio costante della clientela nel corso del rapporto continuativo. Tra queste figurano: l'effettuazione di più ampie ed approfondite verifiche in occasione del compimento da parte del cliente di operazioni considerate a maggior rischio; l'esecuzione periodica dell'attività di customer screening su clienti, beneficiari e soggetti collegati; l'aggiornamento dei dati, informazioni e, conseguentemente, del profilo di rischio della clientela, il monitoraggio della scadenza dei documenti identificativi.

³⁰ Si rimanda alla Procedura IT-CPL-13-IT Monitoraggio delle transazioni e Gestione degli alert (AML/TM), alla nota operativa "AML/CTF Transaction monitoring: Alert management e Attività di controllo" e al Manuale "Gestione segnalazione operazioni sospette" per approfondimento relativamente all'iter di analisi degli alert emersi.



- gli indicatori di anomalia forniti dalla 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);
- il Regolamento IVASS;
- linee guida GAFI per un approccio basato sul rischio per le Compagnie assicurative autorizzate all'esercizio dei rami vita ("*Guidance for a Risk-Based Approach for the Life Insurance Sector*");
- gli Orientamenti congiunti ai sensi dell'articolo 17 e dell'articolo 18, paragrafo 4, della direttiva (UE) 2015/849 emanati dall'ESAs Joint Committee sui fattori che gli enti creditizi e gli istituti finanziari dovrebbero prendere in considerazione nel valutare i rischi.

Si specifica che il sistema di *transaction monitoring* è volto al monitoraggio delle operazioni "ex-post" ed è pertanto da ritenersi complementare ai controlli ex ante intesi quali Blocchi Sospensivi. "Adeguata verifica e valutazione del rischio della clientela". Infatti, da entrambi può prendere avvio l'iter di segnalazione di operazione sospetta, come descritto nell'apposita normativa interna³¹.

Per ciascun indicatore è stata prodotta una scheda di dettaglio che riporta:

- la principale fonte normativa di riferimento;
- la descrizione sintetica dell'evento anomalo che si vuole intercettare nonché la regola di calcolo che permette la generazione dell>alert;
- gli approfondimenti da condurre a seguito della generazione dell>alert. Inoltre, sono fornite delle indicazioni circa le caratteristiche che deve possedere l'operazione anomala intercettata dall'indicatore per ritenersi non sospetta. Alternativamente, è necessario avviare l'iter di segnalazione di operazione sospetta, motivandone le ragioni.

Si riporta una descrizione sintetica delle operazioni intercettate da parte del sistema di transaction monitoring:

- somma degli importi dei premi inferiori a 15.000 euro versati negli ultimi 180 giorni superiore alla soglia di segnalazione;
- somma dei premi nell'ultima settimana inferiore alla soglia di segnalazione, a fronte di importi rilevanti pagati negli ultimi 30 o 180 giorni;
- alta frequenza di versamenti negli ultimi 30 giorni tutti sotto la soglia di rilevazione per le frazionate;
- importo del premio unico dell'operazione maggiore della media dei premi unici pagati nell'ultimo anno;
- riscatti anticipati;
- recesso;
- riscatti con applicazione di penali;
- cambio contraenza;
- designazione dello stesso beneficiario su più polizze;
- lo stesso soggetto è beneficiario/percipiente di liquidazioni relative a molteplici polizze con contraente diverso;
- lo stesso soggetto è percipiente di liquidazioni relative a molteplici polizze con beneficiario diverso;
- operazioni disposte da persona delegata dal cliente;
- numerose sottoscrizioni con soggetto terzo-pagatore diverso da contraente;
- numerose sottoscrizioni fuori piano e numerosi riscatti parziali;
- movimentazione del rapporto non giustificata dall'attività del cliente;
- rimborso parziale di una polizza effettuato poco dopo l'apertura;

³¹ Cfr. Manuale operativo "Attività da eseguire per l'invio delle segnalazioni in caso di operazioni sospette". In aggiunta, il processo di segnalazione di operazioni sospette è descritto anche nella "Politica Antiriciclaggio".

- cliente con domicilio/ residenza in paese a rischio;
- prelevamento di ingenti somme con richiesta di numerosi assegni di importo poco inferiore ai limiti di legge;
- ripetute operazioni di elevato ammontare su rapporti intestati a soggetti minori o di età elevata, ed esecutore diverso da contraente;
- ripetuti pagamenti per importi complessivi rilevanti a favore di più soggetti diversi;
- prelievo di significativo ammontare successivo a investimento su rapporto dormiente;
- operazioni di sottoscrizione ripetute o di importo significativo con provvista proveniente da paesi a rischio;
- frequenti operazioni di sottoscrizione seguite da operazioni di riscatto;
- riscatti con bonifici destinati a soggetti diversi;
- sottoscrizioni con bonifici provenienti da soggetti diversi;
- sottoscrizione negli ultimi 60 giorni di più polizze sulla vita della medesima persona (assicurato);
- cambio del contraente poco prima del pagamento;
- liquidazione della prestazione in paese a rischio;
- coerenza profilo reddituale/patrimoniale;
- verifica coerenza capacità economica.

Si evidenzia che tali indici sono sempre sottoposti a costante revisione e implementazione, anche a seguito delle risultanze dei controlli.

I parametri dell'algoritmo attuale sono dettagliati nell'Allegato 3 - Regole_Operazioni Sospette_KYC4.

XI. Gestione delle operazioni sospette

È disposto che si provveda a **inviare alla UIF prima del compimento dell'operazione 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 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.

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 KYC** 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.
- **Unusual Activity Reports:**
 - Segnalazione interna/ Whistleblowing antiriciclaggio;
 - Profili di rischio alti elaborati dal tool KYC;
 - Riscontro positivo con un nominativo presente nelle liste di sorveglianza;
 - Anomalie rinvenute nell'ambito dello svolgimento dell'adeguata verifica rafforzata.
- **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;
 - 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).

La rilevazione di un'operazione sospetta è il risultato di un **processo³² 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 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 all'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;

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"

- 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 (vedi *supra*), 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.

XII. Controlli di primo e secondo livello

Con riferimento ai controlli di primo e secondo livello, sono previsti sia dei:

- controlli "ex ante" che tramite "blocchi" a sistema su front end BNL e/o attivazione di "blocchi sospensivi" (vedi paragrafo 8.3.2) consentono approfondimenti su specifiche operazioni e/o clienti, sia
- controlli ex post tra i quali³³:
 - controlli svolti dall'unità CCRM (Compliance & Control Risk Management) interna alla funzione Compliance denominati "Generic Control Plan". Questi controlli verificano la corretta applicazione delle procedure relative alla due diligence della clientela, degli intermediari e del processo relativo alle operazioni sospette;
 - controlli svolti dal team Control & Reporting, alcuni dei quali svolti con il supporto delle risorse facenti parte del team KYC & Alert Management, che mirano alla verifica dell'adeguatezza dei processi e dell'efficacia dei presidi della Compagnia in materia antiriciclaggio, antiterrorismo e rispetto delle sanzioni finanziarie internazionali. Nello specifico, il team citato svolge attività di controllo per appurare, fra l'altro, (i) la correttezza del processo di costituzione dossier, (ii) l'efficacia della gestione del processo di alert management e (iii) la regolare esecuzione delle attività in materia di screening;
 - controllo di "quality assurance" svolto dall'unità Regulatory Controls che, con riferimento alle analisi di primo livello a supporto delle operazioni sospette, ha lo scopo di verificare che gli alert oggetto della analisi condotte nel mese precedente siano stati legittimamente archiviati al primo livello ovvero scalati al secondo; le risultanze di tale esercizio sono contenute in un articolato report mensile condiviso con la Funzione Antiriciclaggio.
 - monitoraggio condotto dalla struttura Customer Service e condiviso con la Funzione Antiriciclaggio volto alla individuazione e rendicontazione dei c.d. "scarti" generati a livello di Archivio Unico Informatico rispetto: (i) ai flussi informativi ricevuti dall'Intermediario (in particolare l'individuazione delle anomalie legate al caricamento di dati errati e/o mancanti all'interno del Questionario Due Diligence per operazioni di emissione e/o post vendita); (ii) a disallineamenti/carenze di comunicazione con i sistemi di Portafoglio (NAIS, Foremast etc.).

³³ Per ulteriori approfondimenti circa i controlli dovuti dalla Funzione Compliance e dall'Ufficio Regulatory & Controls, si rimanda alla "Politica Antiriciclaggio" specificatamente al paragrafo 3.2.5.



XIII. OBBLIGHI DI CONSERVAZIONE

11.1 Conservazione dei documenti

La Compagnia conserva i documenti, 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 conservano 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;
- i dati identificativi del cliente, del titolare effettivo e dell'esecutore e le informazioni sullo scopo e la natura del rapporto o della prestazione;
- la data, l'importo e la causale dell'operazione;
- i mezzi di pagamento utilizzati.

I documenti, i dati e le informazioni acquisiti sono conservati per un periodo di 10 anni dalla cessazione del rapporto continuativo. Il sistema di archiviazione della documentazione adottato consente di rendere gli stessi prontamente disponibili, in formato cartaceo o elettronico, su richiesta delle Autorità competenti.

Al fine di permettere a Cardif Vita di essere conforme al dettato normativo, gli operatori acquisiscono copia di tutti i documenti utilizzati per eseguire le attività di adeguata verifica, nonché dei documenti aggiuntivi raccolti e delle verifiche effettuate attraverso fonti esterne. Pertanto:

- il questionario antiriciclaggio della clientela viene inserito nel fascicolo di polizza, assieme ai documenti raccolti per espletare gli obblighi di adeguata verifica;
- la documentazione da acquisire nel caso in cui il cliente sia ritenuto fortemente esposto al rischio di riciclaggio e finanziamento del terrorismo (documentazione aggiuntiva) viene inviata alla Funzione Antiriciclaggio. Alla stessa viene inviata eventuale altra documentazione su richiesta.

In aggiunta, la rete distributiva conserva presso le proprie sedi la documentazione acquisita in fase di instaurazione del rapporto continuativo/ esecuzione di operazioni, mettendola a disposizione delle stesse imprese ogni qual volta ne facciano richiesta.

Cardif Vita, inoltre, si avvale, per la conservazione della documentazione acquisita nell'ambito dell'adeguata verifica del partner o di un fornitore esterno³⁴. Quest'ultimo provvede all'archiviazione in forma cartacea dei documenti pervenuti e alla successiva scansione degli stessi, affinché possano essere prontamente disponibili sulle piattaforme web utilizzate dalle stesse imprese. Il fornitore, inoltre, esegue un controllo circa la completezza della documentazione inviategli dalle imprese. Di seguito la tabella riporta la tipologia di documentazione conservata presso ciascun partner:

Tipologia di prodotto distribuito		Archiviazione
BNL Protection		
Sottoscrizione		Archivio Compagnia presso Microdata
Post-vendita		Archivio Compagnia presso Microdata
BNL Saving		
Sottoscrizione		Archivio Compagnia presso Microdata
Post-vendita		Archivio Compagnia presso Microdata
BNL Previdenza		

³⁴ Il fornitore esterno è Microdata ovvero Previnet in relazione alla tipologia di prodotto sottoscritto.

Tipologia di prodotto distribuito	Archiviazione
Sottoscrizione	Archivio Compagnia presso Previnet
Post-vendita	Archivio Compagnia presso Previnet

Altri Partner Protection	
Sottoscrizione	Archivio intermediari
Post-vendita	Archivio Compagnia presso Microdata

Gestione della clientela diretta	
Emissioni e post-vendita	Archivio Compagnia presso Microdata

11.2 Conservazione dei dati e delle informazioni

Al fine di osservare gli obblighi prescritti dal Decreto antiriciclaggio e dal Regolamento in materia di conservazione dei dati e delle informazioni, la Compagnia fa ricorso all'Archivio Unico Informatico (AUI), intendendo lo stesso quale sistema "equivalente" per l'assolvimento dell'obbligo di conservazione, in attesa dell'emanazione dell'apposito provvedimento regolamentare da parte dell'Autorità di Vigilanza di sistema. In aggiunta all'Archivio Unico Informatico, dati ed informazioni sono conservati all'interno dei Portafogli e del tool KYC.

La compagnia assolve agli obblighi di conservazione dei dati e delle informazioni previsti dal decreto antiriciclaggio attraverso sistemi di conservazione informatizzati che devono assicurare, tra l'altro:

- l'accessibilità completa e tempestiva ai dati e alle informazioni da parte della Banca d'Italia, della UIF o di altra Autorità competente;
- l'acquisizione tempestiva da parte dei destinatari dei documenti, 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;
- l'adozione di idonee misure finalizzate a prevenire qualsiasi perdita dei dati e delle informazioni;
- la trasparenza, la completezza e la chiarezza dei dati e delle informazioni nonché il mantenimento della storicità dei medesimi.

I destinatari completano l'acquisizione dei documenti, dei dati e delle informazioni nei sistemi di conservazione informatizzati tempestivamente e, in ogni caso, non oltre il trentesimo giorno dall'instaurazione del rapporto continuativo, dall'esecuzione dell'operazione, dalla variazione e dalla chiusura del rapporto continuativo:

- I destinatari adempiono gli obblighi di conservazione dei documenti, dei dati e delle informazioni in relazione ai rapporti continuativi e alle operazioni che rientrano nella propria attività istituzionale.
- I dati e le informazioni relativi a rapporti continuativi e alle operazioni sono conservati per i dieci anni successivi alla chiusura del rapporto o al compimento dell'operazione.

Al fine di osservare gli obblighi prescritti dal Decreto antiriciclaggio in riferimento alla "conservazione" e nel periodo transitorio sino all'avvenuta pubblicazione dell'emanando Regolamento in materia di conservazione dei dati e delle informazioni, la Compagnia provvede ad assolvere l'obbligo mediante utilizzo all'Archivio Unico Informatico (AUI), quale Archivio Standardizzato, intendendo lo stesso quale sistema "equivalente" per l'assolvimento dell'obbligo di conservazione.

Tale scelta è stata assunta a seguito di preventiva valutazione di conformità alle disposizioni normative, altresì, considerando che i dati e le informazioni antiriciclaggio sono, parimenti, conservati ed accessibili all'interno del Portafoglio e di AUI (che alimentano la KYC attraverso procedure informatiche di riconoscimento, analisi e transcodifica).

La Funzione Antiriciclaggio, verifica l'affidabilità del sistema informativo di alimentazione dell'AUI, attraverso i controlli svolti dalla Funzione di I livello (Ufficio Regulatory Controls), volti a garantire la consistenza dei dati contenuti nei sistemi gestionali e gli eventi trasmessi in AUI, avvalendosi dell'utilizzo di strumenti diagnostici.



Ai sensi dell'articolo 33 del Decreto antiriciclaggio, la Compagnia provvede all'invio mensile all'UIF dei dati aggregati (cd. flussi S.A.R.A.) concernenti la propria operatività, al fine di consentire le effettuazioni di analisi mirate a far emergere eventuali fenomeni di riciclaggio o di finanziamento del terrorismo nell'ambito di determinate zone territoriali. Specifica attenzione è posta al riscontro di richieste o comunicazioni della UIF circa eventuali anomalie statistiche (c.d. rilievi) che dovessero essere riscontrate.

La soluzione tecnologica implementata dalla Compagnia per garantire la registrazione in AUI è incentrata sull'applicativo WINTAR che provvede a:

- acquisire, a partire da tutte le procedure informatiche che elaborano dati rilevanti ai fini antiriciclaggio, i diversi flussi informativi necessari alla valorizzazione dei dati all'interno dell'AUI;
- eseguire controlli preventivi sui dati, al fine di verificarne la correttezza e consistenza prima della registrazione all'interno dell'Archivio definitivo.

I documenti, i dati e le informazioni acquisiti sono conservati per un periodo di n. 10 anni dalla cessazione del rapporto continuativo, o dall'esecuzione dell'operazione occasionale. Successivamente, i dati dei rapporti e delle operazioni vengono cancellati, ad esclusione motivata dei rapporti (e operazioni) che siano passibili di indagini e/o di richieste delle Autorità e/o siano in contenzioso, per cui i rapporti necessitano di essere conservati fino all'estinzione dell'indagine, della richiesta e/o del procedimento.

XIV. 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. Riguarda inoltre tutto il personale della Compagnia.

A tal proposito, la formazione in ambito antiriciclaggio e di contrasto al finanziamento del terrorismo viene erogata 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").

In particolare, la formazione in materia di 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 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.

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 anche degli ulteriori corsi di tipo manageriale, comportamentale e tecnico finalizzati al rafforzamento delle relative competenze specifiche richieste dall'attività svolta.

Più in particolare la Funzione Antiriciclaggio, ad evento, e con il supporto di consulenti esterni promuove ed organizza sessioni formative dedicate alla disamina ed approfondimento delle principali novità normative e regolamentari in materia di lotta al riciclaggio e al finanziamento del terrorismo e dei relativi impatti sul mestiere assicurativo.

Inoltre, con riferimento alla rete distributiva diretta della Compagnia, la stessa 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 ed agli obblighi antiriciclaggio.

La Funzione Compliance formalizza in specifici *report* la formazione fruita dal personale, in base alle periodicità stabilite dal Gruppo nonché porta all'attenzione del Consiglio di Amministrazione della Compagnia annualmente, nell'ambito del consuntivo del piano di formazione aziendale, i risultati delle formazioni pianificate.



XV. Appendix: Acronimi/Definizioni

ALLINEAMENTO ANAGRAFICO	-	Flusso informatico giornaliero e ad evento che permette l'acquisizione da parte della Compagnia dei dati (inclusi quelli rilevanti ai fini AML / CFT) raccolti dal Partner BNL.
ADV	Adegua ta Verifica	Processo di conoscenza della relazione con il cliente così come prescritto dalla normativa. Consiste nelle seguenti attività: - o identificazione del cliente, del beneficiario e dell'eventuale esecutore; - o identificazione dell'eventuale titolare effettivo del cliente e del beneficiario; - o verifica dell'identità del cliente, del beneficiario, dell'eventuale esecutore e dell'eventuale titolare effettivo del cliente e del beneficiario, sulla base di documenti, dati o informazioni ottenuti da una fonte affidabile e indipendente; acquisizione e valutazione di informazioni sullo scopo e sulla natura del rapporto continuativo e, se rilevante secondo un approccio fondato sul rischio, dell'operazione occasionale; e) esercizio di un controllo costante nel corso del rapporto continuativo.
ADV – MISURE RAFFORZATE	-	Obblighi di adeguata verifica della clientela di cui agli articoli 24 e 25 del decreto antiriciclaggio
ADV – MISURE SEMPLIFICATE	-	Gli obblighi di adeguata verifica della clientela di cui all'articolo 23 del decreto antiriciclaggio
AML / CFT	Anti-Money Laundering / Combating the Financing of Terrorism	L'Antiriciclaggio è l'insieme dei presidi a contrasto del rischio di riciclaggio come definito dall'art. 2 D: Lgs. n. 231/07, in specie si consideri che ricomprende: - 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 criminosa o da una partecipazione a tale attività; - l'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza, al momento della loro ricezione, che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività; - la partecipazione ad uno degli atti di cui ai punti precedenti, l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolare l'esecuzione ed espressamente include anche i cd. "rischi fiscali".
AUI	Archivio Informatico Unico	Archivio, 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 di identificazione.



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.
BLOCCO SOSPENSIVO	-	Blocco informatico automatico (per le operazioni intermedie da BNL) o manuale (per le operazioni gestite direttamente dalla Compagnia) che sospende ex ante l'operazione richiesta dal cliente che presenta una elevata esposizione al rischio di riciclaggio e/o finanziamento del terrorismo, permettendo, in tal modo, di effettuare preliminarmente gli opportuni approfondimenti.
CLIENTE	-	Il soggetto che, anche mediante co-intestazione, instaura rapporti continuativi ovvero compie operazioni (anche quale esecutore) con le imprese o con le imprese stabilite senza succursale
CONTRASTO AL 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
CSR	Corporate Responsibility List Social Exclusion	La CSR Exclusion List, redatta dal Corporate Social Responsibility Department del Gruppo BNP Paribas, che elenca le società e/o i prodotti in riferimento a cui BNP Paribas esclude ogni operatività
DATI IDENTIFICATIVI	-	Dati identificativi del Cliente, del beneficiario, del titolare effettivo (sia esso titolare effettivo sub 2) ovvero sub 3) 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, gli estremi del documento di identificazione, il codice fiscale del beneficiario e, ove ne sia prevista l'assegnazione, anche del relativo titolare effettivo e dell'esecutore
DECRETO ANTIRICICLAGGIO	-	D. Lgs. n. 231 del 21 novembre 2007 modificato dal D. Lgs. n. 90 del 25 maggio 2017 e dal D. Lgs. n. 125 del 4 ottobre 2019 quest'ultima contenente disposizioni attuative della Direttiva (UE) 2018/843
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
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



GROUP RISK ASSESSMENT	-	Annuale valutazione dei rischi di compliance di Gruppo, all'interno della quale viene dedicato uno specifico modulo "fs-Compass", al processo di KYC e, più in generale, del rischio di riciclaggio
IVASS	Istituto per la Vigilanza sulle Assicurazioni	Autorità di Vigilanza nei confronti delle Imprese di Assicurazioni
KYC	Know Your Customer/ Adeguate 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 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	-	Trasmissione o movimentazione di mezzi di pagamento indipendentemente dalla connessione con un rapporto continuativo, nonché la designazione di uno o più beneficiari specificamente individuati o univocamente individuabili
ORIENTAMENTI	-	Orientamenti congiunti, indirizzati alle autorità competenti degli Stati membri 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
PEP	Politically Exposed Person/ Persone politicamente esposte	Art. 1 comma 9 lettera dd) del D. Lgs.90/2017: 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. Include anche la categoria dei PIL (Persone Importanti Localmente) come individuate dalla normativa regolamentare di settore, quali soggetti che per esercizio di cariche, funzioni o attività con la Pubblica Amministrazione, seppure non possano essere ricompresi nell'ambito della classificazione di PEPs debbano essere equiparati ai PEPs.
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
PROTECTION	-	Indica l'attività della Compagnia che riguarda la vendita di prodotti diversi da IBIPs (Insurance Based Investment Products). Cfr. anche Protezione.
PROTEZIONE	-	Indica l'attività della Compagnia che riguarda la vendita di prodotti diversi da IBIPs (Insurance Based Investment Products). Cfr. anche Protection.
QDD	Questionario di due diligence	Modulo utilizzato per la raccolta delle informazioni rilevanti ai fini AML da parte della clientela. Cfr. anche SAV.
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
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 specie
RISPARMIO	-	Indica l’attività della Compagnia che riguarda la vendita di prodotti IBIPs (Insurance Based Investment Products). Cfr. anche Saving.
SAV	Scheda di adeguata verifica	Modulo utilizzato per la raccolta delle informazioni rilevanti ai fini AML da parte della clientela. Cfr. anche QDD.
SAVING	-	Indica l’attività della Compagnia che riguarda la vendita di prodotti IBIPs (Insurance Based Investment Products). Cfr. anche Risparmio.
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

