



consip

**Divisione Risorse Umane e Comunicazione
Area Risorse Umane, Organizzazione e Processi**

Policy per il governo dei rischi di riciclaggio e di finanziamento del terrorismo

Versione 1.0

Classificazione documento: Consip Public

21 settembre 2020



DATA	VERSIONE	DESCRIZIONE	CAP. /SEZ. MODIFICATI
21/09/2020	1.0	Nascita documento	Tutti

Storia del documento

	DATA	AREA/FUNZIONE	DIVISIONE
Redatto da:	18/06/2019	Gestore della segnalazione delle operazioni sospette (Gestore SOS) Compliance	- DCS
Verificato da:	17/09/2020		DCS
	16/09/2020		DRC
Approvato da:	17/09/2020	AD	

Emissione del documento

Il contenuto del presente documento è stato oggetto di delibera da parte del CdA in data 18/06/2019



Indice

1.	INTRODUZIONE	4
1.1	SCOPO E CAMPO DI APPLICAZIONE.....	4
1.2	COMPLIANCE NORMATIVA.....	4
1.3	RIFERIMENTI INTERNI.....	4
1.4	ACRONIMI E GLOSSARIO.....	5
2.	GOVERNO DEI RISCHI DI RICICLAGGIO E DI FINANZIAMENTO DEL TERRORISMO	8
2.1	PREMESSA.....	8
2.1.1	Gli obblighi antiriciclaggio per le Pubbliche Amministrazioni	8
2.1.2	Gli indicatori di anomalia per la segnalazione di operazione sospetta	8
2.1.3	Profili sanzionatori.....	9
2.2	MAPPATURA E VALUTAZIONE DEI RISCHI DI RICICLAGGIO.....	9
2.3	SEGNALAZIONI DI OPERAZIONI SOSPETTE.....	10
2.3.1	Linee guida e principi generali.....	10
2.3.2	Ruoli e responsabilità	11
2.3.3	Strumenti a supporto.....	13
2.3.4	Il processo di segnalazione di operazione sospetta.....	13
2.3.5	Presidi di controllo e flussi informativi	15
2.3.6	Presidi di controllo e flussi informativi	15



1. INTRODUZIONE

1.1 SCOPO E CAMPO DI APPLICAZIONE

La *Policy* definisce le linee guida per la gestione dei rischi di riciclaggio e di finanziamento del terrorismo presso la Società, tenuto conto delle disposizioni normative e regolamentari vigenti e delle *best practice* di settore.

La *Policy*, in particolare, delinea:

- i principi generali e le linee guida per la prevenzione, la mitigazione e la gestione del rischio di riciclaggio e di finanziamento al terrorismo;
- i ruoli e le responsabilità degli Organi e delle altre funzioni aziendali;
- i processi di gestione e presidio del rischio di riciclaggio e di finanziamento del terrorismo;
- il sistema di reporting e di gestione dei flussi informativi tra il gestore SOS e la UIF, gli Organi e le altre funzioni aziendali.

Il presente documento e i successivi aggiornamenti – laddove sostanziali - sono approvati e adottati con delibera del Consiglio di Amministrazione della Società.

Il Gestore SOS, con il supporto della Divisione Compliance e Societario, cura l'aggiornamento della *Policy* nel caso in cui si verificano variazioni di rilievo nella disciplina di riferimento, ovvero nell'organizzazione aziendale, sottoponendola all'approvazione di cui sopra nel caso intervengano modifiche sostanziali. Il Gestore SOS e la Divisione Compliance e Societario operano, inoltre, affinché la Società adotti procedure, conformi alla presente *Policy*, aventi ad oggetto la gestione delle segnalazioni delle operazioni sospette.

1.2 COMPLIANCE NORMATIVA

Di seguito si riportano le normative applicabili al processo.

Normativa	Settore
Decreto Legislativo 21 novembre 2007 n. 231	Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione e successive modifiche e integrazioni
Decreto Legislativo 22 giugno 2007 n. 109	Misure per prevenire, contrastare e reprimere il finanziamento del terrorismo e l'attività dei Paesi che minacciano la pace e la sicurezza internazionale, in attuazione della direttiva 2005/60/CE e successive modifiche e integrazioni
Comunicazioni UIF del 18 aprile 2016 e del 13 ottobre 2017	Comunicazioni per la prevenzione del finanziamento del terrorismo internazionale
Istruzioni UIF del 23 aprile 2018	Comunicazioni di dati e informazioni concernenti le operazioni sospette da parte degli uffici delle Pubbliche Amministrazioni.

1.3 RIFERIMENTI INTERNI

[R1] Procedura per la segnalazione di operazioni sospette



1.4 ACRONIMI E GLOSSARIO

ACRONIMI

AML	Anti Money Laundering
CdA	Consiglio di Amministratore
CFT	Countering the Financing of Terrorism
DCS	Divisione Compliance e Societario
DRC	Divisione Risorse Umane e Comunicazione
GAFI	Gruppo di Azione Finanziaria Internazionale
O.E.	Operatore Economico
PEP	Persona Politicamente Esposta
RTI	Raggruppamento Temporaneo d'Impresa
SOS	Segnalazione di Operazione Sospetta
UIF	Unità di Informazione Finanziaria

GLOSSARIO

Applicativo informatico	applicativo informatico implementato dalla Società per la gestione dei controlli ai fini antiriciclaggio e per la gestione dell'iter di segnalazione di operazione sospetta
Approccio basato sul rischio (<i>Risk based approach</i>)	principio sulla base del quale, la Società commisura il rigore delle misure antiriciclaggio al rischio di riciclaggio desumibile dalla natura e dalle caratteristiche dei clienti, dalle tipologie di prodotto o servizio richieste, dall'area geografica di riferimento, nonché da qualsiasi altro elemento utile a fini di valutazione
Decreto	il Decreto Legislativo 21 novembre 2007, n. 231 e successive modifiche e integrazioni
Finanziamento del terrorismo	qualsiasi attività diretta, con ogni mezzo, alla fornitura, alla raccolta, alla provvista, all'intermediazione, al deposito, alla custodia o all'erogazione, in qualunque modo realizzate, di fondi e risorse economiche, destinati a essere, direttamente o indirettamente, in tutto o in parte, utilizzabili 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 sopra riportate
Gestore della segnalazione delle operazioni sospette (Gestore SOS)	soggetto individuato all'interno della Pubblica Amministrazione con provvedimento formalizzato e incaricato dal CdA di (i) valutare, alla luce di tutti gli elementi disponibili, le operazioni sospette provenienti dalle funzioni aziendali o di cui sia venuto altrimenti a conoscenza nell'ambito della propria attività, (ii) trasmettere alla UIF le segnalazioni ritenute fondate, omettendo l'indicazione



	<p>dell'identità dei soggetti coinvolti nella procedura di segnalazione dell'operazione, (iii) informare dell'esito della propria valutazione, il responsabile di primo livello che ha dato origine alla segnalazione laddove provenga dalle funzioni aziendali, assicurando la tutela della riservatezza e (iv) mantenere evidenza delle valutazioni effettuate nell'ambito della procedura, anche in caso di mancato invio della segnalazione alla UIF</p>
Operazione sospetta	<p>operazione che per caratteristiche, entità, natura o qualsivoglia altra circostanza conosciuta in ragione delle funzioni esercitate, tenuto conto della capacità economica e dell'attività svolta dal soggetto cui è riferita, induca a ritenere, in base agli elementi disponibili e alle valutazioni svolte, che il denaro, i beni, o le utilità oggetto dell'operazione possono provenire dai delitti di riciclaggio e di finanziamento del terrorismo</p>
Paesi terzi ad alto rischio	<p>Paesi non appartenenti all'Unione Europea i cui ordinamenti presentano carenze strategiche nei rispettivi regimi nazionali di prevenzione del riciclaggio e del finanziamento del terrorismo, per come individuati dalla Commissione Europea nell'esercizio dei poteri di cui agli articoli 9 e 64 della direttiva e dal GAFI</p>
Persone Politicamente Esposte (PEPs)	<p>le persone fisiche indicate all'articolo 1, comma 2, lettera dd) del Decreto</p>
Personale	<p>i dipendenti e coloro che operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione della Società, anche in forma diversa dal rapporto di lavoro subordinato</p>
Principio di proporzionalità	<p>principio sulla base del quale, la Società definisce i presidi in termini di organizzazione, procedure e controlli interni in coerenza con la propria forma giuridica, le sue dimensioni, la propria articolazione organizzativa, le sue caratteristiche e con la complessità delle attività svolte</p>
Pubbliche Amministrazioni	<p>come disciplinate dall'art. 1, comma 2, lettera hh) del Decreto, "le amministrazioni pubbliche di cui all'art. 1, comma 2, del D. Lgs. 165/2001, e successive modificazioni, gli enti pubblici nazionali, le società partecipate dalle amministrazioni pubbliche e dalle loro controllate, ai sensi dell'art. 2359 del codice civile, limitatamente alla loro attività di pubblico interesse disciplinata dal diritto nazionale o dall'Unione europea nonché i soggetti preposti alla riscossione dei tributi nell'ambito della fiscalità nazionale o locale, quale che ne sia la forma giuridica"</p>
Riciclaggio	<p>a) la conversione o il trasferimento di beni, effettuati essendo a conoscenza che essi provengono da un'attività criminosa o da una partecipazione a tale attività, allo scopo di occultare o dissimulare l'origine illecita dei beni medesimi o di aiutare chiunque sia coinvolto in tale attività a sottrarsi alle conseguenze giuridiche delle proprie azioni; b) l'occultamento o la dissimulazione della reale natura, provenienza, ubicazione, disposizione, movimento, proprietà dei beni o dei diritti sugli stessi, effettuati essendo a conoscenza che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività; c) l'acquisto, la detenzione o l'utilizzazione di beni essendo a conoscenza, al momento della loro</p>



ricezione, che tali beni provengono da un'attività criminosa o da una partecipazione a tale attività; d) la partecipazione ad uno degli atti di cui alle lettere a), b) e c) l'associazione per commettere tale atto, il tentativo di perpetrarlo, il fatto di aiutare, istigare o consigliare qualcuno a commetterlo o il fatto di agevolare l'esecuzione

Rischio di riciclaggio

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

Sanction lists sensibili a fini antiterrorismo

liste dei soggetti che siano collegabili alle organizzazioni terroristiche, che minacciano la pace e la sicurezza internazionale ovvero che siano oggetto di sanzioni finanziarie da parte dell'Unione Europea o dalle autorità americane, designati rispettivamente dal Consiglio di Sicurezza dell'ONU, dall'Unione Europea, dai decreti del Ministero dell'Economia e delle Finanze, nonché di quella dell'Office of Foreign Asset Control (OFAC) degli Stati Uniti

Unità di Informazione Finanziaria

istituita presso la Banca d'Italia, acquisisce 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



2. GOVERNO DEI RISCHI DI RICICLAGGIO E DI FINANZIAMENTO DEL TERRORISMO

2.1 PREMESSA

2.1.1 Gli obblighi antiriciclaggio per le Pubbliche Amministrazioni

Il Decreto all'art. 10 sancisce l'applicazione di specifici obblighi in ambito antiriciclaggio per le Pubbliche Amministrazioni competenti allo svolgimento di compiti di amministrazione attiva o di controllo, nell'ambito dei seguenti procedimenti o procedure:

- procedimenti finalizzati all'adozione di provvedimenti di autorizzazione o concessione;
- procedure di scelta del contraente per l'affidamento di lavori, forniture e servizi secondo le disposizioni di cui al codice dei contratti pubblici;
- procedimenti di concessione ed erogazione di sovvenzioni, contributi, sussidi, ausili finanziari, nonché attribuzioni di vantaggi economici di qualunque genere a persone fisiche ed enti pubblici e privati.

Nello specifico, le Pubbliche Amministrazioni sono tenute a:

- adottare procedure interne, proporzionate alle proprie dimensioni organizzative e operative, idonee a valutare il livello di esposizione dei propri uffici al rischio di riciclaggio e finanziamento del terrorismo cui sono esposti nell'esercizio della propria attività istituzionale e indicare le misure necessarie a mitigarlo;
- comunicare alla UIF dati e informazioni concernenti le operazioni sospette di cui vengono a conoscenza nell'esercizio della propria attività istituzionale;
- adottare, nel quadro dei programmi di formazione continua del personale, misure idonee a formare il personale sugli obblighi previsti dalla normativa antiriciclaggio e in particolare ad assicurare il riconoscimento, da parte dei propri dipendenti, delle fattispecie meritevoli di essere comunicate alla UIF al fine di consentire lo svolgimento di analisi finanziarie mirate a far emergere fenomeni di riciclaggio e di finanziamento del terrorismo.

In attuazione di quanto previsto dal Decreto, in data 23 aprile 2018 la UIF ha emanato apposite istruzioni sulle comunicazioni di dati e informazioni concernenti le operazioni sospette da parte degli uffici delle Pubbliche Amministrazioni, con l'obiettivo di individuare i dati e le informazioni da trasmettere, le modalità e i termini della relativa comunicazione nonché gli indicatori per agevolare la rilevazione delle operazioni sospette.

2.1.2 Gli indicatori di anomalia per la segnalazione di operazione sospetta

La UIF individua specifici indicatori di anomalia volti a ridurre i margini di incertezza delle valutazioni soggettive connesse alle comunicazioni di operazioni sospette e con lo scopo di contribuire al contenimento degli oneri e alla correttezza e omogeneità delle comunicazioni medesime.

Gli indicatori di anomalia riguardano l'attività istituzionale in concreto svolta dalla Società e sono connessi (i) all'identità o comportamento del soggetto cui è riferita l'operazione, (ii) alle modalità di richiesta o esecuzione delle operazioni e (iii) con i settori di attività. Sulla base di tale *framework*, la Società ha individuato gli indicatori concretamente applicabili alla propria attività istituzionale e ha, inoltre, definito ulteriori indicatori sulla base del contesto in cui opera.



Gli indicatori di anomalia – individuati dalla UIF e dalla Società - sono un ausilio nell'individuazione di operazioni potenzialmente sospette, tuttavia anche in considerazione della continua evoluzione delle modalità di svolgimento delle operazioni, non possono essere considerati esaustivi.

Pertanto anche in assenza di tali indicatori è necessario porre la massima attenzione con riferimento a ulteriori comportamenti e caratteristiche dell'operazione che sono egualmente sintomatici di profili di sospetto.

D'altro canto, la mera ricorrenza di operazioni o comportamenti descritti in uno o più indicatori di anomalia non è motivo di per sé sufficiente per la qualificazione dell'operazione come sospetta ai fini della comunicazione alla UIF; è in ogni caso necessario svolgere una specifica analisi nel concreto e una valutazione complessiva dell'operatività avvalendosi di tutte le altre informazioni disponibili.

Gli indicatori di anomalia sono analizzati in relazione a:

- circostanze oggettive, quali ad esempio la ripetitività dei comportamenti o la rilevanza economica dell'operazione, l'elevata complessità dell'attività;
- circostanze soggettive, quali ad esempio l'assenza di giustificazione economica, l'inusualità o illogicità dell'operazione ovvero l'eventuale incoerenza della giustificazione adottata o dell'attività / profilo economico-patrimoniale del soggetto cui è riferita l'operazione.

Le comunicazioni alla UIF devono essere effettuate anche in caso di sospetto di operazioni riconducibili al finanziamento del terrorismo. In tal senso, con riguardo anzitutto al riscontro del nominativo e dei relativi dati anagrafici nelle *Sanctions list* sensibili ai fini antiterrorismo, non è in ogni caso sufficiente, ai fini della comunicazione, la mera omonimia del nominativo.

2.1.3 Profili sanzionatori

L'inosservanza della normativa in materia di antiriciclaggio costituisce illecito disciplinare ed è sanzionabile in base al Sistema Disciplinare definito da Consip S.p.A. che definisce la tipologia e le modalità di applicazione delle sanzioni.

2.2 MAPPATURA E VALUTAZIONE DEI RISCHI DI RICICLAGGIO

L'identificazione e la valutazione periodica del livello di esposizione della Società al rischio di riciclaggio e finanziamento del terrorismo, in relazione all'esercizio della propria attività istituzionale, assume un ruolo cruciale nell'ambito di un modello di gestione del rischio.

In particolare, essa risulta funzionale:

- all'articolazione dei principi di approccio basato sul rischio e di proporzionalità in funzione dei quali organizzare il sistema dei presidi interni a prevenzione dei rischi in materia;
- all'individuazione e programmazione degli interventi correttivi aventi l'obiettivo di mitigare il livello di rischio nel concreto rilevato.

In tale contesto, la Società si è dotata di una metodologia integrata di analisi e valutazione dei rischi che consente di ottenere un unico modello di gestione dei rischi aziendali: il *risk assessment* integrato relativamente ai rischi di cui al d.lgs. 231/01 (responsabilità amministrativa degli enti), alla L. 190/12 (anticorruzione), al d.lgs. 33/2013 (trasparenza), al d.lgs. 262/2005, al d.lgs. 231/2007 (antiriciclaggio) e al Regolamento UE/2016/679 (privacy).



I principali benefici derivanti da tale approccio sono l'utilizzo di una metodologia unica di analisi e valutazione dei rischi e dei controlli, la razionalizzazione e integrazione dei rischi e controlli, un Risk Model complessivo e tematico per famiglie di rischio, le sinergie tra organi di controllo.

Il *risk assessment* integrato è condotto utilizzando una metodologia *risk based e process oriented*: ciascun evento di rischio è ricondotto al relativo macro processo, processo, fase e attività, così da ottenere la completa cartografia dei rischi aziendali.

Tutti gli eventi di rischio individuati sono stati catalogati in dieci famiglie di rischio tra le quali la famiglia di rischio "antiriciclaggio". A ciascun evento di rischio mappato nella famiglia "antiriciclaggio" è stato attribuito un *risk scoring* residuo e inerente basato sulla valutazione di due parametri: "impatto" e "probabilità di accadimento".

2.3 SEGNALAZIONI DI OPERAZIONI SOSPETTE

2.3.1 Linee guida e principi generali

In applicazione dell'approccio basato sul rischio (c.d. *risk based approach*) e in coerenza con il principio di proporzionalità, la Società assicura un'azione di prevenzione e di contrasto al riciclaggio e al finanziamento del terrorismo coerente con l'articolazione societaria, la complessità e la dimensione aziendale, la tipologia dei servizi e prodotti offerti e le caratteristiche della clientela servita tramite l'adozione dei seguenti presidi minimi:

- definizione di politiche per la gestione complessiva del rischio di riciclaggio;
- chiara definizione di ruoli, compiti e responsabilità in capo a ciascun presidio organizzativo;
- sistemi organizzativi e procedure idonei a garantire l'osservanza degli obblighi di segnalazione delle operazioni sospette;
- esercizio di un'attività di controllo sul rispetto delle procedure interne adottate e degli obblighi di legge e regolamentari in materia di antiriciclaggio.

Ai fini del rispetto degli obblighi di collaborazione attiva, la Società comunica tempestivamente alla UIF dati e informazioni concernenti le operazioni in relazione alle quali abbia il sospetto o motivi ragionevoli per sospettare che siano in corso o che siano state compiute o tentate attività di riciclaggio o di finanziamento del terrorismo o che comunque i fondi, indipendentemente dalla loro entità, provengano dal compimento di un'attività criminosa.

Il sospetto può essere desunto da qualsiasi figura aziendale, alla luce di una compiuta valutazione degli elementi oggettivi e soggettivi acquisiti nell'ambito dell'attività istituzionale svolta (ad esempio, caratteristiche, entità e natura delle operazioni, loro collegamento o qualsivoglia altra circostanza conosciuta, tenuto conto anche della capacità economica e dell'attività svolta dal soggetto). Il sospetto è desunto a prescindere dall'importo e dalla rilevanza dell'operazione.

La segnalazione non è subordinata alla creazione di un quadro indiziario di riciclaggio da parte del segnalante. La segnalazione è subordinata soltanto a un giudizio puramente tecnico di valutazione degli elementi oggettivi e soggettivi che caratterizzano le operazioni.

Il ruolo della Pubblica Amministrazione nella segnalazione di operazione sospetta è pertanto preventivo e non repressivo, interpretato con metodi di analisi finanziaria e non inquirente.

La Società monitora la presenza di eventuali elementi di sospetto in tutti gli ambiti che costituiscono l'attività istituzionale della Società con riferimento ai processi di gara. La Società monitora inoltre a titolo prudenziale eventuali anomalie inerenti ai pagamenti contabili.



Al fine di agevolare l'individuazione delle operazioni sospette, la Società fa riferimento agli indicatori di anomalia emanati e periodicamente aggiornati dalla UIF. Partendo da tale *framework* e considerando l'attività istituzionale in concreto svolta dalla Società, sono state individuate le fattispecie di rischio da tenere in considerazione da parte delle funzioni aziendali per la rilevazione di possibili situazioni anomale o comportamenti atipici.

Le comunicazioni sono inoltrate al Gestore SOS per il tramite di un applicativo informatico dedicato che garantisce omogeneità nell'esecuzione degli adempimenti operativi, tracciabilità delle verifiche svolte e monitoraggio dei tempi di esecuzione.

La comunicazione è inviata in via telematica alla UIF, anche quando si dispone di dati e informazioni inerenti a operazioni rifiutate o interrotte ovvero eseguite in tutto o in parte presso altri destinatari di autonomi obblighi di segnalazione.

È fatto divieto a tutto il personale, ove in possesso dell'informazione, di dare comunicazione al/ai soggetto/i segnalato/i alla UIF o a terzi dell'avvenuta segnalazione o di notizie ad essa relative, fatti salvi gli adempimenti operativi previsti dal processo interno di segnalazione delle operazioni sospette.

Al fine di garantire efficacia e riservatezza nella gestione delle informazioni, la UIF considera il Gestore SOS quale proprio interlocutore per tutte le comunicazioni e i relativi approfondimenti.

La Società adotta tutte le misure idonee a tutelare la riservatezza dell'identità delle persone coinvolte nel processo di segnalazione di una operazione sospetta. Il nominativo del segnalante può essere rivelato solo quando l'Autorità giudiziaria, con decreto motivato, lo ritenga indispensabile ai fini dell'accertamento di reati per i quali è stato avviato il procedimento.

2.3.2 Ruoli e responsabilità

Al fine di mitigare il rischio di riciclaggio e di finanziamento del terrorismo, risulta imprescindibile il coinvolgimento degli Organi aziendali (Consiglio di Amministrazione e Collegio Sindacale) e il corretto adempimento degli obblighi previsti dalla normativa vigente.

Il Consiglio di Amministrazione approva il modello adottato per la gestione del processo di segnalazione di operazioni sospette e fornisce al Gestore SOS idonei strumenti per la gestione e il corretto funzionamento dello stesso. Inoltre, il Consiglio di Amministrazione assegna al Gestore SOS idonei e adeguati poteri per lo svolgimento dell'incarico assicurandogli autonomia e indipendenza nell'espletamento dello stesso.

Nello specifico il Consiglio di Amministrazione:

- approva la *Policy* per il governo dei rischi di riciclaggio e di finanziamento del terrorismo riportate nel presente documento e i successivi aggiornamenti, laddove intervengano modifiche sostanziali al documento;
- cura l'attuazione degli indirizzi strategici e delle politiche di governo del rischio di riciclaggio;
- approva, su proposta del Gestore SOS, la procedura per la segnalazione delle operazioni sospette volta ad assicurare l'omogeneità dei comportamenti, la tracciabilità del processo, la tutela della riservatezza dei soggetti coinvolti nella procedura di segnalazione e l'adozione di adeguati strumenti, anche informatici, per la rilevazione delle operazioni anomale;
- approva i programmi di formazione del personale sugli obblighi previsti dalla disciplina in materia di antiriciclaggio.

Il Collegio Sindacale è tenuto a comunicare tempestivamente al Gestore SOS le operazioni anomale di cui viene a conoscenza nell'esercizio delle proprie funzioni.



Il Gestore SOS è nominato e revocato dal Consiglio di Amministrazione; egli non ha responsabilità dirette di aree operative né è gerarchicamente dipendente da soggetti di queste aree. Il ruolo del Gestore SOS è adeguatamente formalizzato e reso pubblico all'interno della Società e la nomina e la revoca del medesimo Gestore sono comunicate tempestivamente alla UIF con le modalità indicate dalla stessa Autorità.

Il Gestore delle segnalazioni di operazioni sospette:

- valuta, alla luce di tutti gli elementi disponibili, le operazioni sospette provenienti dalle funzioni aziendali o di cui sia venuto altrimenti a conoscenza nell'ambito della propria attività;
- trasmette alla UIF le segnalazioni ritenute fondate, omettendo l'indicazione dell'identità dei soggetti coinvolti nella procedura di segnalazione dell'operazione;
- informa dell'esito della propria valutazione la funzione aziendale che ha dato origine alla segnalazione, assicurando la tutela della riservatezza;
- mantiene evidenza delle valutazioni effettuate nell'ambito della procedura, anche in caso di mancato invio della segnalazione alla UIF;
- propone alla Società l'adozione di tutte le misure necessarie ad assicurare l'efficacia del sistema dei controlli antiriciclaggio.

Egli svolge le proprie attività con autonomia di giudizio e riservatezza anche nei confronti delle altre funzioni aziendali e, ai fini dell'espletamento dei propri compiti:

- ha libero accesso ai flussi informativi concernenti la prevenzione del riciclaggio e del finanziamento del terrorismo diretti agli Organi aziendali e alle funzioni aziendali coinvolte a vario titolo nell'assetto dei presidi organizzativi antiriciclaggio;
- utilizza, ai fini di valutazione, anche eventuali elementi desumibili da fonti informative liberamente accessibili;
- è tenuto a conoscere e applicare con rigore ed efficacia le istruzioni, gli schemi e gli indicatori emanati di volta in volta dalla UIF nell'ambito delle sue prerogative;
- svolge un ruolo di interlocuzione unitaria con le Autorità e risponde tempestivamente alle eventuali richieste di approfondimento provenienti dalla UIF.

Per lo svolgimento delle proprie attività, il Gestore SOS si avvale della Divisione Internal Audit e della Divisione Compliance e Societario, per quanto di rispettiva competenza.

La Divisione Compliance e Societario supporta il Gestore SOS nella valutazione delle operazioni sospette ritenute meritevoli di attenzione, conducendo analisi inerenti aspetti di conformità, di natura legale e reputazionale. La Divisione monitora, inoltre, periodicamente la composizione della lista dei Paesi a rischio in ambito AML¹ e, in caso di variazioni, informa il Gestore SOS.

La Divisione Internal Audit supporta il Gestore SOS nella valutazione delle operazioni sospette ritenute meritevoli di attenzione, conducendo verifiche rafforzate volte a valutare il livello di coinvolgimento della Società in possibili episodi di riciclaggio o di finanziamento del terrorismo ed esegue le attività previste dal piano integrato dei controlli a fini di verifica di funzionalità dell'assetto dei presidi interni.

Il personale, ciascuno nell'ambito delle proprie attribuzioni e competenze, è tenuto ad operare nel rispetto degli obblighi di legge e ad assicurare la corretta attuazione delle politiche di gestione del rischio di riciclaggio e di finanziamento del terrorismo. Il personale è responsabile, per quanto di propria competenza, nell'ambito delle mansioni attribuite, della segnalazione tempestiva ai soggetti competenti

¹ Si fa riferimento ai paesi individuati come ad alto rischio rispettivamente dalla Commissione Europea e dal GAFI.



di ogni circostanza per la quale sanno, sospettano, o hanno ragionevoli motivi per sospettare che siano state compiute, tentate o siano in corso operazioni di riciclaggio, di finanziamento del terrorismo o che i fondi, indipendentemente dalla loro entità, provengano da un'attività criminosa.

In ogni caso, il personale si attiene alle indicazioni impartite dalla documentazione interna in materia di antiriciclaggio e antiterrorismo e partecipa ai programmi di formazione definiti dalla Società.

2.3.3 Strumenti a supporto

La Società ha adottato - in relazione alle diverse fasi di cui si compone un processo di gara - un applicativo informatico dedicato per la gestione dell'intero *iter* di segnalazione di operazione sospetta (fasi di rilevazione delle operazioni anomale, analisi e valutazione delle fattispecie evidenziate, inoltro delle segnalazioni sospette all'Autorità di Vigilanza, trasmissione del feedback al soggetto segnalante).

Tale applicativo, oltre a garantire l'adozione di un processo guidato di segnalazione di operazione sospetta (es. processo organizzato in fasi successive, con presenza di blocchi che non consentono lo sviluppo della lavorazione in assenza del completamento delle attività di cui alle fasi precedenti), assicura inoltre:

- l'omogeneità nell'esecuzione degli adempimenti operativi;
- la tracciabilità delle verifiche svolte;
- il monitoraggio dei tempi di esecuzione;
- l'inoltro delle comunicazioni in via telematica;
- la riservatezza dell'identità delle persone che segnalano le operazioni e del contenuto delle medesime.

2.3.4 Il processo di segnalazione di operazione sospetta

In applicazione dell'approccio basato sul rischio e in coerenza con il principio di proporzionalità, la Società adotta presidi commisurati al livello di rischio rilevato e gradua, sulla base di margini di autonomia e discrezionalità, l'intensità di strumenti e controlli.

In particolare, il modello operativo definito per la gestione delle segnalazioni di operazioni sospette si basa sulla graduazione dell'intensità e della frequenza delle verifiche da condurre, in funzione delle soglie (importi di base d'asta) relative ai bandi di gara, delle fasi in cui si articola il lotto di gara e delle tipologie di operatori economici coinvolti.

L'obiettivo in tal senso è quello di attivare controlli maggiormente pervasivi, rispettivamente, nei bandi di gara con importi di base d'asta sopra soglia, nelle fasi di gara che coincidono con l'aggiudicazione e la stipula del contratto e nei confronti degli operatori economici aggiudicatari e relativi soggetti consorziati / organizzati sotto forma di raggruppamenti temporanei di impresa.

2.3.4.1 Il processo "guidato" di segnalazione di operazione sospetta

Per la gestione del processo di segnalazione di operazioni sospette, in relazione ai diversi bandi pubblicati dalla Società, essa adotta un modello dedicato che si articola su tre macro-fasi:

- la prima fase (cd. rilevazione di operazioni anomale) prevede il coinvolgimento delle funzioni di primo livello (tipicamente rappresentate da strutture che svolgono controlli di natura



amministrativa / tecnica / economica ovvero verifiche di tipo amministrativo / contabile) ed è caratterizzata da:

- compilazione di apposite 'checklist' all'interno di un applicativo informatico. La compilazione di tali 'checklist' all'interno dell'applicativo è richiesta per ogni fase in cui si articola la procedura di gara² (distinta per ciascun lotto) ed è finalizzata, a fronte delle attività eseguite, alla rilevazione di eventuali fattispecie di anomalia a fini antiriciclaggio e antiterrorismo;
- lavorazione di appositi 'alert' all'interno di un applicativo informatico, generati (anche in funzione del livello di rischio associato alle fattispecie di anomalie rilevate all'interno del medesimo applicativo in sede di compilazione delle 'checklist' in relazione a singoli operatori economici ovvero ad operatori economici diversi ma coinvolti nella medesima offerta) a fronte di un possibile sospetto che siano in corso o che siano state compiute o tentate operazioni di riciclaggio o di finanziamento del terrorismo. La lavorazione dell'"alert" si conclude, in caso di conferma del sospetto, con avvio dell'iter segnalatico mediante compilazione di apposito 'modulo' ovvero, in caso di mancata conferma del sospetto, con archiviazione motivata della segnalazione;
- compilazione, in caso di conferma del sospetto, di apposito 'modulo' all'interno di un applicativo informatico. La compilazione di tale 'modulo' è funzionale all'avvio dell'iter segnalatico;
- la seconda fase (cd. valutazione delle fattispecie di anomalia rilevate) prevede il coinvolgimento di una figura di primo livello gerarchico (tipicamente rappresentata dal Responsabile della Divisione di riferimento) ed è caratterizzata dalla compilazione di una sezione dedicata del 'modulo' all'interno dell'applicativo informatico.

La compilazione di tale sezione ha l'obiettivo di valutare la fondatezza degli elementi di sospetto rinvenuti dalle funzioni di primo livello, ai fini del successivo inoltro o meno dell'operazione anomala nei confronti del Gestore SOS;

- la terza fase (cd. analisi delle segnalazioni sospette) prevede il coinvolgimento del Gestore SOS ed è caratterizzata dalla compilazione di una sezione dedicata del 'modulo' all'interno di un applicativo informatico.

In particolare, il Gestore conduce, anche mediante il supporto della Divisione Internal Audit e della Divisione Compliance e Societario, controlli rafforzati inerenti profili di conformità e legali nonché il possibile coinvolgimento della Società in episodi di riciclaggio, volti a valutare la

² La compilazione all'interno dell'applicativo informatico della checklist è in particolare prevista, con frequenza ad evento, nelle fasi di:

- ricezione delle offerte, in relazione agli operatori economici partecipanti (e relativi soggetti consorziati / organizzati sotto forma di raggruppamenti temporanei di impresa) e alle relative offerte presentate con riferimento al medesimo lotto di gara;
- lavori di commissione, in relazione alle offerte presentate nel medesimo lotto di gara;
- aggiudicazione del contratto, in relazione all'operatore economico aggiudicatario (e relativi soggetti consorziati / organizzati sotto forma di raggruppamenti temporanei di impresa);
- stipula del contratto, in relazione all'operatore economico aggiudicatario;
- (eventuale) coinvolgimento di operatori economici in qualità di subappaltatori, in relazione agli operatori coinvolti.
- esecuzione del contratto, in relazione all'operatore economico aggiudicatario. La compilazione all'interno dell'applicativo informatico di tale checklist è prevista con frequenza periodica - almeno annuale - ed in ogni caso in sede di chiusura del contratto).

È possibile che sulla base dell'evento del processo di gara gestito, non tutte le fasi sopra menzionate siano presenti (es. nelle gare negoziate sono presenti le sole fasi di aggiudicazione e stipula del contratto).



fondatezza degli elementi di sospetto rinvenuti dalle funzioni di primo livello e dalla figura di primo livello gerarchico, ai fini del successivo inoltro o meno della comunicazione nei confronti dell'UIF. Al termine del processo segnaletico, il Gestore SOS comunica - con modalità idonee ad assicurare la tutela della riservatezza - l'esito della propria valutazione alla funzione che ha dato origine alla segnalazione (figura di primo livello gerarchico e/o funzione di primo livello).

2.3.4.2 Il processo "spontaneo" di segnalazione di operazione sospetta

Tutto il personale dipendente è tenuto a segnalare eventuali situazioni di anomalia o comportamenti atipici di cui viene a conoscenza nell'ambito delle proprie attività, a prescindere dalla presenza di 'alert' generati dall'applicativo informatico dedicato.

A titolo esemplificativo, la presenza di situazioni di sospetto può essere rilevata anche in relazione a fattispecie operative che esulano dai processi di gara (quali ad esempio mancata riconciliazione degli incassi ricevuti dagli operatori economici; ricezione di incassi superiori a quelli effettivamente dovuti).

In tali casi, è prevista - da parte delle funzioni interessate - la compilazione extra - procedura del 'modulo' cartaceo ai fini dell'avvio dell'iter segnaletico.

Il processo segnaletico può essere attivato anche da parte del Gestore SOS qualora egli sia venuto a conoscenza - nell'ambito della propria attività - di determinate fattispecie di rischio.

In tali casi, è prevista:

- se la segnalazione è inerente a un processo di gara, la compilazione di iniziativa del 'modulo' all'interno dell'applicativo informatico; l'iter segnaletico non prevede ulteriori fasi di valutazione;
- se la segnalazione è inerente a un'attività che esula il processo di gara, a compilazione del 'modulo' extra procedura.

2.3.5 Presidi di controllo e flussi informativi

La Società esegue in maniera periodica verifiche, richiamate all'interno del piano integrato dei controlli, volte a valutare l'efficacia dei presidi adottati al fine di mitigare e gestire i rischi di riciclaggio di denaro e di finanziamento del terrorismo.

All'esito di tali controlli, sono individuati gli interventi di adeguamento e le attività di monitoraggio da porre in essere, al fine di apportare delle soluzioni alle anomalie, carenze e/o criticità emerse.

Nell'ottica di condividere le informazioni necessarie allo svolgimento effettivo e consapevole dei compiti loro affidati con frequenza almeno annuale, tra il Gestore SOS, gli Organi aziendali (Consiglio di Amministrazione e Collegio Sindacale) e le funzioni di controllo interessate (Organismo di Vigilanza, Responsabile della prevenzione della corruzione e della trasparenza e Divisione Internal Audit) sono previsti flussi informativi sotto forma di (i) relazioni periodiche inerenti le attività poste in essere, gli esiti dei controlli effettuati e le eventuali azioni di mitigazione individuate e (ii) reportistica ad evento a fronte di richieste di chiarimento / approfondimento.

2.3.6 Presidi di controllo e flussi informativi

Nella consapevolezza che un'efficace applicazione della normativa antiriciclaggio presuppone la piena conoscenza delle sue finalità, dei relativi principi, degli obblighi e delle responsabilità da essa derivanti e in ottemperanza a quanto richiesto dall'art. 10 comma 5 del Decreto, la Società realizza specifici programmi di formazione del personale sugli obblighi previsti dalla normativa antiriciclaggio e di contrasto



al finanziamento del terrorismo, al fine di diffondere tra i propri dipendenti una cultura del rischio di riciclaggio e di sensibilizzare tutto il personale sulle problematiche connesse a tale rischio.

Annualmente viene sottoposto all'approvazione del Consiglio di Amministrazione un Piano di Formazione concernente anche gli obblighi previsti dalla normativa antiriciclaggio.

La formazione è finalizzata a conseguire un aggiornamento su base continuativa dei dipendenti e dei collaboratori al fine di garantire la preparazione in merito agli obblighi di segnalazione delle operazioni sospette; sono inoltre previsti focus specifici sull'evoluzione del rischio di riciclaggio e sugli schemi tipici delle operazioni finanziarie criminali.