Standard professionale RICS

Standard e linee guida professionali RICS, globali

Lotta alla corruzione e all'abuso d'ufficio, al riciclaggio di denaro e al finanziamento del terrorismo

1a edizione, febbraio 2019

rics.org/guidance

Lotta alla corruzione, all'abuso d'ufficio, al riciclaggio di denaro e al finanziamento del terrorismo

Standard professionale RICS

1a edizione, febbraio 2019

Pubblicato da Royal Institution of Chartered Surveyors (RICS)

Parliament Square

London

SW1P 3AD

www.rics.org

Prodotto dal RICS Commercial Property Professional Group.

ISBN 978 1 78321 369 6

Indice

Ringraziamenti ..... **iv**
Standard e linee guida professionali RICS **1**
Standard professionale RICS 1
Glossario **3**
Prefazione **5**
Parte 1: Requisiti **6**
1.1 Panoramica generale 6
1.2 Applicazione 6
1.3 Corruzione e abuso d'ufficio 6
1.4 Riciclaggio di denaro e finanziamento del terrorismo 7
Parte 2: Linee guida **9**
2.1 Corruzione e abuso d'ufficio 9
2.2 Riciclaggio di denaro e finanziamento del terrorismo 10
Parte 3: Linee guida supplementari **12**
3.1 Rischi di corruzione e abuso d'ufficio 12
3.2 Rischi di riciclaggio di denaro e finanziamento del terrorismo 12
3.3 Affidamento 14
3.4 Deroghe 14
3.5 Approccio basato sul rischio 15
3.6 Adeguata verifica rafforzata (AVR) e Adeguata verifica semplificata (AVS) 15
3.7 Tutore della compliance e dell'etica 16
3.8 Codice di condotta 16
3.9 Persone politicamente esposte 17
3.10 Titolarità effettiva 17
3.11 Whistleblowing 18
Riferimenti **19**
Approfondimenti **20**
Appendici **21**
Appendice A **22**
Modello del modulo di due diligence del cliente 22
Appendice B **23**
Bozza dei controlli in materia di compliance in capo all'azienda 23
Bozza della richiesta di informazioni relativa alla titolarità effettiva 23
Checklist antiriciclaggio 25
Appendice C **26**
Modello della lettera di affidamento 26

Ringraziamenti

RICS ringrazia per il contributo ai presenti standard professionali.

Autore tecnico:

Alex Ktorides (Inces Gordon Dadds)

Ringraziamenti speciali a Benjamin Atkins e James Fraser

Gruppo di lavoro:

Andrea Amadesi FRICS (APREA)

Alexander Aronsohn FRICS (RICS)

Nigel Astbury MRICS (Christie and Co)

Peter Bolton-King FRICS (RICS)

Caitriona de Burca (Sherry Fitzgerald)

Gillian Dixon (Gerald Eve)

Frances Forsyth (Arcadis)

Raquel Loll (RICS)

Vicky Moss (BNP Paribas Real Estate)

Ilana Rosenzweig (RICS)

Thijs Stoffer (ICREA)

Cyril Troyanov (Altenburger Ltd)

Jo Upton MRICS (Pegasi)

Richard Watson MRICS

Responsabile del Gruppo Professionale RICS:

Nigel Sellars FRICS (RICS)

Ringraziamenti speciali:

Jon Bowey MRICS

RICS Publishing:

Standards Publishing Manager: Antonella Adamus

Project Manager: Ellie Scott

Editor: Sean Agass

RICS ringrazia per il loro contributo alla traduzione italiana:

Revisione tecnica:

Giulia Comparini MRICS

Daniele Levi Formìggini MRICS (coordinatore del gruppo)

Francesca Prandi MRICS

RICS Italia:

Paola Sanzeni, Country Manager

RICS Publishing:

Georgia Brambilla, Translations Manager

Standard e linee guida professionali RICS

Standard professionali RICS

Definizione e ambito di applicazione

Gli Standard professionali RICS precisano i requisiti di prassi per i professionisti e le aziende soggetti alla regolamentazione da parte di RICS. Con l'espressione standard professionale si intende uno standard professionale o personale per le finalità del Codice deontologico RICS.

Disposizioni in materia di good practice vs. prassi obbligatoria

Le sezioni all'interno degli standard professionali che utilizzano il verbo "dovere" al tempo indicativo presente (deve/devono) stabiliscono requisiti professionali, comportamentali, di competenza e/o requisiti tecnici, che hanno natura obbligatoria per i membri.

Le sezioni all'interno degli standard professionali che utilizzano il verbo "dovere" al tempo condizionale presente (dovrebbe/dovrebbero) rappresentano le aree di good practice. RICS riconosce che potrebbero sussistere circostanze eccezionali nelle quali sia appropriato per un membro derogare a queste disposizioni; in tali circostanze RICS potrebbe richiedere al membro di giustificare le proprie decisioni e azioni.

Applicazione di queste disposizioni nei procedimenti legali o disciplinari

Nei procedimenti amministrativi o disciplinari, RICS terrà conto degli standard professionali pertinenti nel decidere se un membro abbia agito in modo professionale, appropriato e con congrue competenze. È anche probabile che durante un qualsiasi procedimento giudiziario, un giudice, arbitro o equivalente tenga conto dei requisiti professionali RICS.

RICS riconosce che potrebbero sussistere obblighi di legge o standard regionali, nazionali o internazionali che abbiano la precedenza sugli standard professionali RICS.

Definizione dello status dei documenti

La tabella seguente illustra le categorie di contenuti professionali RICS e le rispettive definizioni.

Tipo di documento	Definizione
Codice deontologico RICS per i Membri (RICS Rules of Conduct for Members) e *Codice deontologico RICS per le Aziende (RICS Rules of Conduct for Firms)*	Questi Codici precisano gli standard di condotta e prassi professionale a cui devono attenersi i professionisti e le aziende soggetti alla regolamentazione da parte di RICS.
Standard internazionale	Standard di alto livello sviluppato in collaborazione con altri organi competenti.
Standard professionale RICS (PS)	**Requisito obbligatorio per i professionisti e le aziende soggetti alla regolamentazione da parte di RICS.**
Linea guida (GN) RICS	Documento contenente raccomandazioni o metodologie relative alle buone pratiche consolidate, adottate da professionisti competenti e rigorosi.
Codice RICS sulla buona prassi (CoP)	Documento sviluppato in collaborazione con altre organizzazioni professionali e stakeholder che avrà lo status di standard professionale o linea guida.
Guida RICS per la giurisdizione	Fornisce informazioni sul mercato locale di pertinenza associate a uno standard internazionale RICS o uno standard professionale RICS. Ciò comprende la legislazione, le associazioni e le organizzazioni professionali locali nonché qualsiasi altra informazione utile che aiuti l'utente a comprendere i requisiti locali connessi allo standard. Non si tratta di linee guida o di materiale per le best practice, ma piuttosto di informazioni a supporto dell'adozione e implementazione degli standard a livello locale.

Glossario

Le definizioni seguenti fanno riferimento al presente standard professionale e non comprendono questioni giuridiche o di altra natura, così come definite in relazione agli obblighi di legge o normativi locali.

Abuso d'ufficio: l'uso improprio di pubblici uffici o poteri a fini di lucro privato o l'uso improprio del potere privato in relazione alle prassi e prestazioni commerciali.

Adeguata conoscenza: la comprensione appropriata delle questioni e delle risposte connesse alla corruzione, all'abuso d'ufficio, al riciclaggio di denaro e al finanziamento del terrorismo, in modo tale che la persona fisica possa applicare i requisiti di questo standard professionale al proprio ruolo. Questo livello di conoscenza varierà a seconda del settore e dell'organizzazione in cui la persona fisica opera e del ruolo che la stessa ricopre. Tale conoscenza può essere acquisita mediante la frequentazione di percorsi formativi, studi privati o sulla base dell'esperienza lavorativa.

Adeguata verifica del cliente/Conosci il tuo cliente (know your customer/client - KYC): l'adozione di misure appropriate per accertare chi sia il cliente e, ove pertinente, il rispettivo titolare effettivo finale e la controparte. Tali misure possono tradursi in controlli relativamente semplici volti a verificare l'identità del cliente o possono comportare indagini più approfondite. In molti paesi si tratta di un obbligo di legge e normativo.

Affidamento: la misura secondo cui i controlli richiesti sulle persone fisiche o sulle società sono stati condotti da terzi con esito soddisfacente, il che significa che non devono essere ripetuti.

Cartello di monopolio di fissazione dei prezzi: un gruppo di produttori di beni o servizi formalmente indipendenti, il cui obiettivo sia quello di aumentare i proventi collettivi spingendo al livello più alto possibile il prezzo di tali beni o servizi (o eventualmente fissare, imporre, scontare o stabilizzare i prezzi), generalmente ottenendo proventi per tutti i venditori.

Corruzione: l'offerta, la promessa, la concessione, la richiesta o l'accettazione di un vantaggio come incentivo ad un'azione illegale, non etica o una violazione della fiducia.

Evento scatenante: un evento che implica che un'azienda rivaluti il livello di rischio di un cliente, partner, fornitore esterno o dipendente, e potenzialmente conduca un'adeguata verifica rafforzata.

Finanziamento del terrorismo: la richiesta, la raccolta o la concessione di fondi con l'intenzione che possano essere utilizzati a supporto di atti od organizzazioni terroristiche. I fondi stanziati direttamente o indirettamente a tale fine costituiscono finanziamento del terrorismo.

Indicatori di allerta: caratteristiche comuni che considerate sia singolarmente che congiuntamente potrebbero indicare il potenziale abuso del settore immobiliare per finalità di riciclaggio di denaro o finanziamento del terrorismo.

Leggi applicabili: le leggi e i regolamenti locali e globali applicabili alle aziende e alle persone fisiche. Questi possono dipendere dalla località in cui è ubicata la sede principale, dal luogo in cui il presunto abuso d'ufficio o atto di corruzione viene commesso o ricevuto, o dal paese in cui è registrata la capogruppo.

Pagamento di agevolazione: un pagamento effettuato a favore di un funzionario di governo con l'obiettivo di velocizzare un atto amministrativo di routine. Tali pagamenti sono abituali ed ammessi dalla legge in alcuni paesi, ma in molte giurisdizioni si configurano come reati.

Persona di controllo rilevante (PSC): una persona fisica o un soggetto giuridico che eserciti controllo o influenza significativo su una società. Tale controllo e influenza possono essere esercitati in molti modi diversi, ad esempio la persona fisica gode del diritto di veto assoluto sulle decisioni relative alla gestione della società.

Persona politicamente esposta (PEP): una persona fisica, e i familiari di tale persona fisica, alla quale sono state affidate funzioni pubbliche di primo piano da un qualsiasi paese od organizzazione internazionale. Rientrano in questa definizione capi di Stato o di governo, politici di alto livello, alti funzionari governativi, giudiziari o militari, alti dirigenti di società statali e direttori, vicedirettori e membri del consiglio di amministrazione o aventi funzioni equivalenti in seno ad organizzazioni internazionali. Le PEP che rinuncino alle proprie cariche o i loro parenti che cessino di essere membri della famiglia (ad esempio, in seguito a divorzio) non saranno più considerati come tali 12 mesi dopo il verificarsi di tali eventi.

Riciclaggio di denaro: l'azione di nascondere la fonte dei proventi di attività criminali per mascherarne la provenienza illegale. Questo potrebbe avvenire occultando, trasferendo e/o riciclando denaro illecito o altra valuta per mezzo di una o più operazioni, o convertendo i proventi di attività criminali in beni apparentemente legittimi.

Riciclatori di denaro professionisti: coloro che si specializzano nel mettere i criminali in condizione di evadere le salvaguardie in materia di antiriciclaggio di denaro e lotta al finanziamento del terrorismo e le relative sanzioni. Svolgono tale funzione dietro commissione o provvigione. Ad esempio, consulenti fiscali, legali o contabili che agiscono in veste di facilitatori professionisti per i criminali.

Schema: un'operazione o un caso specifico di riciclaggio di denaro o finanziamento del terrorismo che associa varie tecniche, meccanismi e strumenti in una sola struttura.

Segnalazione: l'adozione di misure appropriate per richiamare l'attenzione su attività note o presunte che implichino questioni di riciclaggio di denaro, corruzione o abuso d'ufficio e/o finanziamento del terrorismo. L'azione di segnalazione potrebbe configurarsi come processo interno od esterno e dovrebbe almeno essere conforme alle leggi applicabili, come definite.

Terrorismo: l'uso o la minaccia di violenza per perseguire obiettivi ideologici ad opera di governi, attori non statali o personale sotto copertura che agisce per conto di governi. Il terrorismo non colpisce solo le vittime specificatamente individuate, mirando ad avere ripercussioni su obiettivi che rappresentano uno spettro più ampio della società. Le diverse legislazioni nazionali contengono ciascuna una propria definizione di terrorismo ed elenchi di gruppi di organizzazioni terroristiche individuate.

Titolarità effettiva/Titolare effettivo: chiunque benefici della titolarità di una partecipazione sociale o di un diritto di proprietà, che sia o meno iscritto nei registri come titolare. Sono inoltre compresi coloro che esercitano un controllo effettivo finale sulla persona giuridica o sull'accordo. In molte giurisdizioni, il titolare effettivo è definito come la persona fisica che detiene o controlla il 25% o più delle azioni o degli utili di un soggetto giuridico.

Per ulteriori informazioni su queste definizioni si rimanda al Gruppo di Azione Finanziaria Internazionale (GAFI) al sito **www.fatf-gafi.org**.

Prefazione

In veste di ONG anticorruzione, Transparency International (TI) si prefigge di accrescere la consapevolezza in merito a quali siano i costi sociali, economici e politici della corruzione e sostiene misure concrete per affrontare tale questione. Nei 25 anni dalla costituzione di TI, la corruzione su larga scala è stata sempre più intesa come fenomeno transfrontaliero. La corruzione non coinvolge solo i funzionari pubblici e i privati che pagano le tangenti; spesso necessita anche dell'accesso al sistema finanziario e dell'uso di società di comodo anonime e di facilitatori professionisti che aiutano a riciclare i proventi.

Lungi dall'essere un reato che non provoca vittime, la corruzione inoltre priva le istituzioni statali di risorse estremamente necessarie, che potrebbero essere utilizzate per investimenti nei settori della sanità, dell'istruzione e delle infrastrutture, solo per citarne alcuni.

Negli ultimi anni, si sono moltiplicate le evidenze secondo cui il riciclaggio di denaro per mezzo del settore immobiliare non è un semplice rischio, ma una realtà. La ricerca pubblicata nel 2016 da TI-UK ha individuato 986 proprietà fondiarie londinesi con collegamenti a Persone politicamente esposte, detenute tramite strutture societarie registrate in giurisdizioni segrete. Nel contempo, in Canada, si è riscontrato che 46 delle 100 abitazioni più costose di Vancouver hanno proprietà poco chiare, che utilizzano società di comodo offshore, trust e prestanomi.

Oltre alle criticità dei quadri normativi in materia di antiriciclaggio di denaro che consentono queste ed altre tipologie di proprietà poco chiare, in molti paesi le autorità pubbliche dispongono di risorse insufficienti da dedicare alla vigilanza e alla supervisione. Le valutazioni nazionali condotte dal 2014 in oltre 50 paesi dal Gruppo di Azione Finanziaria Internazionale (GAFI), incaricato della formulazione di standard globali, hanno portato alla luce ripetute lacune istituzionali e giuridiche.

In questo contesto, le misure proattive intraprese dai professionisti del settore immobiliare e finalizzate a rafforzare gli standard, come il presente standard professionale RICS, vengono accolte con favore. In particolare, l'aspettativa di questo standard che i membri e le aziende regolamentate da RICS vadano oltre le disposizioni di legge è di fondamentale importanza, per via delle debolezze strutturali esistenti. Ove realizzate con coerenza, le misure concepite per accrescere la trasparenza, ridurre i rischi e promuovere la fiducia conducono anche a risultati aziendali migliori a livello di settore.

Nel 2017 e 2018, TI ha tratto beneficio direttamente dal contributo di RICS ad un progetto che mira ad accrescere il dialogo tra le autorità, il settore e la società civile per quanto riguarda la realizzazione efficace delle misure in materia di antiriciclaggio di denaro. TI auspica di continuare a collaborare con RICS e a condividere gli insegnamenti che emergono dall'applicazione di questo standard professionale nei confronti dei membri RICS.

– Transparency International, dicembre 2018

25 YEARS TRANSPARENCY INTERNATIONAL the global coalition against corruption

Parte 1: Requisiti

1.1 Panoramica generale

Il presente standard professionale è dedicato alla *corruzione*, all'*abuso d'ufficio*, al *riciclaggio di denaro* e al *finanziamento del terrorismo* ed è suddiviso in tre parti:

1 Requisiti obbligatori per la lotta alla *corruzione*, all'*abuso d'ufficio*, al *riciclaggio di denaro* e al *finanziamento del terrorismo*.

2 Linee guida per la definizione di good practice a supporto della lotta alla *corruzione*, all'*abuso d'ufficio*, al *riciclaggio di denaro* e al *finanziamento del terrorismo*.

3 Linee guida supplementari su alcuni dei concetti di cui alle parti 1 e 2.

I controlli di mitigazione della *corruzione* e dell'*abuso d'ufficio* implicano normalmente attività di monitoraggio della propria organizzazione. Al contempo, la gestione efficace dei rischi di *riciclaggio di denaro e finanziamento del terrorismo* implica il fatto di essere vigili in merito alle azioni compiute dalle parti esterne con le quali i professionisti e le aziende soggetti alla regolamentazione da parte di RICS potrebbero intrattenere rapporti, come i clienti e gli intermediari terze parti che abbiano presentato nuovi o potenziali clienti.

La *corruzione*, l'*abuso d'ufficio*, il *riciclaggio di denaro* e il *finanziamento del terrorismo* sono pratiche illegali e non etiche ed è possibile che nel corso di un'unica operazione vengano commesse più attività tra queste. Si dovrebbe pertanto essere vigili rispetto a questo tipo di attività, condotte sia internamente che esternamente alla propria organizzazione, con clienti e terze parti, e disporre di procedure per identificarle, monitorarle, segnalarle e prevenirle.

Le definizioni dei termini usati nel presente standard professionale sono indicate nel *Glossario*. Tali termini sono scritti in corsivo se usati altrove nel documento.

1.2 Applicazione

Il presente standard professionale si applica a tutti i membri RICS e alle aziende regolamentate da RICS coinvolti nella professione laddove vi sia il potenziale per attività di *corruzione*, *abuso d'ufficio*, *riciclaggio di denaro* e/o *finanziamento del terrorismo*. Laddove lo standard contravvenisse alla legislazione locale, prevarrà quest'ultima.

1.3 Corruzione e abuso d'ufficio

1.3.1 Con riferimento alla corruzione e all'abuso d'ufficio, le **aziende regolamentate da RICS devono**:

- astenersi dall'offrire o dall'accettare, direttamente o indirettamente, qualunque cosa che possa dar luogo ad un atto di *corruzione*;
- adottare piani per essere conformi alle leggi applicabili che disciplinano la *corruzione* e l'*abuso d'ufficio*, e garantire di attenersi a tali piani;
- *segnalare* alle autorità competenti (così come precisate dalla legislazione locale) qualsiasi attività di cui siano a conoscenza che violi le leggi *anticorruzione*; laddove non fosse

applicabile alcuna legislazione locale, l'attività dovrebbe essere registrata e, ove possibile, segnalata a un alto dirigente;

- agire secondo criteri di due diligence nell'effettuare valutazioni periodiche scritte dei rischi che l'azienda affronta e che potrebbero favorire la *corruzione* o l'*abuso d'ufficio*. Nel determinare il livello appropriato di due diligence, l'azienda può prendere in considerazione la tipologia di attività che svolge e l'ambiente in cui opera;
- conservare le informazioni in merito a come l'azienda abbia soddisfatto i requisiti del presente standard professionale.

1.3.2 Con riferimento alla corruzione e all'abuso d'ufficio, i **membri RICS devono**:

- astenersi dall'offrire o dall'accettare, direttamente o indirettamente, qualunque cosa che possa dar luogo ad un atto di *corruzione*;
- assicurare di disporre di un'*adeguata conoscenza* della *corruzione* e dell'*abuso d'ufficio* per essere in grado di attenersi ai requisiti del presente standard professionale;
- segnalare alle autorità competenti (così come precisate dalla legislazione locale) qualsiasi attività di cui siano a conoscenza che violi le leggi *anticorruzione* applicabili; laddove non fosse applicabile alcuna legislazione locale, l'attività dovrebbe essere registrata e, ove possibile, segnalata a un alto dirigente.

1.4 Riciclaggio di denaro e finanziamento del terrorismo

1.4.1 Con riferimento al riciclaggio di denaro e al finanziamento del terrorismo, le **aziende regolamentate da RICS devono**:

- astenersi dal favorire o dall'essere complici di attività di *riciclaggio di denaro* o *finanziamento del terrorismo*;
- adottare sistemi e percorsi formativi per essere conformi a queste leggi e assicurare che vengano osservate;
- *segnalare* alle autorità competenti (così come precisate dalla legislazione locale) qualsiasi sospetto di attività di *riciclaggio di denaro* o *finanziamento del terrorismo*; laddove non fosse applicabile alcuna legislazione locale, l'attività dovrebbe essere registrata e, ove possibile, segnalata a un alto dirigente;
- valutare e rivedere periodicamente i rischi che i rapporti d'affari esistenti o futuri presentano in relazione alla possibile commissione di reati per *riciclaggio di denaro* o *finanziamento del terrorismo*;
- assicurare di rispondere in modo appropriato ai rischi individuati, ivi compresa la conduzione di verifiche appropriate sui clienti;
- fare *affidamento* solo laddove vi sia un livello appropriato di fiducia nella qualità delle informazioni fornite dalle parti terze – si dovrebbe fare *affidamento* solo sulle parti terze che applichino standard conformi ai requisiti di legge, che forniscano all'operatore di mercato soggetto all'obbligo uno scambio completo di tutte le informazioni in materia di lotta al riciclaggio (AML – Anti Money Laundering) legalmente richieste con riferimento alla parte individuata e solo confermando l'identità e la verifica dell'identità del cliente o della controparte in questione. La responsabilità finale per la valutazione del rischio e le azioni intraprese in base alle informazioni di terzi resta in capo al membro o all'azienda regolamentata;
- adottare misure appropriate per identificare il cliente e le finalità dell'operazione;

- verificare l'identità dei clienti intraprendendo controlli dell'identità di base;
- registrare e conservare le informazioni in merito a come l'azienda abbia soddisfatto i requisiti del presente standard professionale.

1.4.2 Con riferimento al *riciclaggio di denaro* e al *finanziamento del terrorismo*, **i membri RICS devono**:

- astenersi dal favorire o dall'essere complici di attività di *riciclaggio di denaro* o *finanziamento del terrorismo*;
- *segnalare* alle autorità competenti (così come precisate dalla legislazione locale) qualsiasi sospetto di attività di *riciclaggio di denaro* o *finanziamento del terrorismo*; laddove non fosse applicabile alcuna legislazione locale, l'attività dovrebbe essere registrata e, ove possibile, segnalata a un alto dirigente.

Parte 2: Linee guida

2.1 Corruzione e abuso d'ufficio

2.1.1 Con riferimento alla *corruzione* e all'*abuso d'ufficio*, le **aziende regolamentate da RICS** dovrebbero:

- redigere una policy scritta in materia di *anticorruzione*, comprensiva di una valutazione del rischio che specifichi nel dettaglio la natura e l'impatto dei rischi sull'attività aziendale - tale policy dovrebbe essere rivista e aggiornata periodicamente in modo appropriato;
- adottare una governance e un sistema di controlli appropriati, proporzionati al tipo di attività svolta dall'azienda;
- incoraggiare la trasparenza in seno all'organizzazione, tenendo un registro dove annotare, a titolo esemplificativo ma non esaustivo:
  - regalie
  - soggiorni, intrattenimento e spese
  - viaggi dei clienti e soggiorni
  - contributi alla politica
  - donazioni a enti di beneficenza e sponsorizzazioni
  - conflitti di interesse potenziali
- fornire al personale linee guida chiare, in modo tale che ciascuno comprenda il proprio ruolo nel prevenire la corruzione e l'abuso d'ufficio e sia consapevole che quanto indicato di seguito non sarà tollerato:
  - i cosiddetti *pagamenti di agevolazione*; sebbene tali pagamenti possano non essere illegali nei paesi in cui vengono eseguiti, essi non dovrebbero essere eseguiti senza aver ottenuto l'autorizzazione esplicita della sede centrale
  - corruzione
  - fissazione dei prezzi finalizzata a creare un monopolio o cartello
  - mancata dichiarazione di un conflitto di interesse
- nominare un referente in seno alla società o alla sede locale per confrontarsi sulle questioni relative alla compliance e alle questioni etiche; le aziende regolamentate di grandi dimensioni potrebbero decidere di nominare formalmente un tutore locale della compliance e dell'etica, il che si configura come best practice per le aziende regolamentate di grandi dimensioni; le aziende di minori dimensioni potrebbero anch'esse decidere in tal senso, a seconda delle implicazioni in termini di risorse;
- pubblicare un codice di condotta e fornirlo al personale;
- condurre verifiche adeguate sui fornitori terzi per assicurare che agiscano in modo appropriato; se previsto dalla legislazione locale in materia di corruzione e abuso d'ufficio verificare che essi agiscano secondo i requisiti applicabili.

2.1.2 Con riferimento alla *corruzione* e all'*abuso d'ufficio*, i **membri RICS** dovrebbero:

- dichiarare alcune voci al datore di lavoro, a titolo esemplificativo ma non esaustivo:
  - regalie
  - soggiorni, intrattenimento e spese
  - viaggi dei clienti e soggiorni
  - donazioni a enti di beneficenza e sponsorizzazioni
- frequentare percorsi formativi pertinenti forniti dal datore di lavoro o da un organismo di autoregolamentazione in materia di *corruzione* e *abuso d'ufficio*;
- avere familiarità e agire in conformità alla policy, alle procedure e al codice di condotta del datore di lavoro in materia di *corruzione* e *abuso d'ufficio*;
- in caso di posizione di senior management, assumere un ruolo guida nell'assicurare che il datore di lavoro adotti un regime appropriato per contrastare i rischi di *corruzione* e *abuso d'ufficio*.

2.2 Riciclaggio di denaro e finanziamento del terrorismo

2.2.1 Con riferimento al *riciclaggio di denaro* e al *finanziamento del terrorismo*, le **aziende regolamentate da RICS** dovrebbero:

- disporre di una policy scritta in materia di *riciclaggio di denaro* e *finanziamento del terrorismo* che riguardi le seguenti questioni:
  - nelle situazioni ad alto rischio in cui sia richiesta un'adeguata verifica rafforzata, la comprensione dell'origine dei fondi di un'operazione
  - l'identificazione delle PEP, delle PSC e di qualsiasi potenziale violazione delle sanzioni
  - il processo a cui attenersi per l'*adeguata verifica del cliente*
  - le situazioni in cui sia appropriato condurre un'adeguata verifica semplificata, un'adeguata verifica standard/ordinaria o un'adeguata verifica rafforzata (si rimanda alla sezione 3.6)
- adottare una governance e un sistema di controlli appropriati, proporzionati al tipo di attività svolta dall'azienda;
- fornire al personale percorsi formativi appropriati e ricorrenti, per assicurare che ciascuno abbia familiarità con i rischi associati al *riciclaggio di denaro* e al *finanziamento del terrorismo* e con i sistemi implementati dall'azienda per contrastare tali rischi;
- mantenere riservate le segnalazioni di qualsivoglia sospetto di attività di *riciclaggio di denaro* e *finanziamento del terrorismo* (per le linee guida in merito al whistleblowing, si rimanda alla sezione 3.11);
- individuare il *titolare effettivo* di una società/un cliente coinvolto in un'operazione;
- nominare una figura senior tra i cui compiti vi sia quello di assicurare l'adozione di policy in materia di *antiriciclaggio di denaro* e *lotta al finanziamento del terrorismo* e la rispettiva osservanza.

2.2.2 Con riferimento al *riciclaggio di denaro* e al *finanziamento del terrorismo*, **i membri RICS** dovrebbero:

- tenersi aggiornati in merito all'attuale percorso formativo offerto dal datore di lavoro o da un organismo di autoregolamentazione in materia di *riciclaggio di denaro* o *finanziamento del terrorismo*;
- attenersi alla policy e alle procedure del datore di lavoro con riferimento al *riciclaggio di denaro* e al *finanziamento del terrorismo*;
- mantenere riservate le segnalazioni di qualsivoglia sospetto di attività di *riciclaggio di denaro* e *finanziamento del terrorismo*;
- in caso di posizione di senior management, assumere un ruolo di leadership facendo in modo di assicurare che il datore di lavoro adotti un regime appropriato per contrastare i rischi di *riciclaggio di denaro* e *finanziamento del terrorismo*.

Parte 3: Linee guida supplementari

3.1 Rischi di corruzione e abuso d'ufficio

È importante che le aziende e le persone fisiche siano a conoscenza dei rischi di *corruzione* e *abuso d'ufficio* a cui devono far fronte nello svolgimento della normale attività lavorativa. La valutazione del rischio può iniziare con un esame delle tipologie di rischi più pertinenti per l'azienda. In genere tali rischi vengono elencati in un registro dei rischi e classificano la buona prassi per le principali attività dell'azienda (in particolare le modalità accettate per ottenere incarichi e svolgerli).

Il livello di rischio dipende spesso dal paese in cui l'attività viene condotta e dalla misura in cui i controlli nazionali sono disponibili e/o applicati. Alcuni paesi e settori generano un rischio superiore rispetto ad altri (si veda, a titolo di esempio, l'indice di percezione della corruzione (*Corruption Perceptions Index*) di Transparency International e gli elenchi dei paesi ad alto rischio pubblicati dal GAFI). Quando l'attività viene condotta in paesi o settori con un rischio superiore, è opportuno disporre di un piano per gestire le questioni che possono derivarne. E' utile prendere in considerazione le modalità con le quali poter condividere le informazioni tra filiali e uffici per operazioni o clienti comuni, al fine di assicurare la corretta individuazione dei rischi.

Le aziende che abbiano constatato che le rispettive attività generano rischi molto contenuti di *corruzione* e *abuso d'ufficio* necessitano di minori controlli rispetto a quelle con rischi superiori, potenzialmente per effetto delle attività che conducono e dei paesi e dei settori in cui operano.

È buona prassi che le aziende che ritengono di avere rischi superiori nominino una persona o un team responsabile della valutazione dei rischi, prima di progettare e testare controlli da mettere in campo con l'obiettivo di mitigare tali rischi. Le aziende che presentano rischi minori dovranno comunque valutare i propri rischi e monitorarli per individuare eventuali cambiamenti. È necessario condurre una revisione periodica al fine di assicurare che i rischi e i controlli continuino ad essere in linea con la valutazione.

A prescindere dall'esposizione al rischio, tutte le aziende devono prevedere regole chiare in merito a quali siano le pratiche accettabili e fissare limiti appropriati di cui tutto il personale sia a conoscenza e ai quali possa accedere facilmente.

Per le aziende con rischi minori, non sono strettamente necessarie policy e procedure molto estese. Per molte aziende, ad eccezione di quelle con rischi superiori, saranno sufficienti dei memorandum per il personale (e gli agenti) su quanto ci si attende dai processi aziendali e la fissazione di una soglia chiara da parte dei dirigenti di ciascuna azienda.

3.2 Rischi di riciclaggio di denaro e finanziamento del terrorismo

I fondi provenienti da *denaro riciclato* vengono spesso "stratificati" per mezzo di un unico pagamento o trasferimento/operazione ovvero per mezzo di una serie di simili movimenti, in modo tale che i proventi possano essere occultati e utilizzati in un secondo momento dall'esecutore.

Tra gli esempi tipici, vi è l'uso dei proventi di un reato per acquistare un bene lecito, come un immobile, detenuto a nome di una persona fisica o di una struttura più complessa, come un trust conforme alle leggi o un gruppo di società. Tale bene viene detenuto e infine utilizzato normalmente o venduto e convertito in strumenti liquidi. È questo il modo in cui i criminali riciclano i proventi e la ragione per la quale le aziende e le persone fisiche sono esposte a un rischio elevato nei settori delle proprietà e degli immobili.

Sapere con chi si intrattengono rapporti d'affari è un primo passo importante per contrastare il *riciclaggio di denaro* e il *finanziamento del terrorismo*. I requisiti delle procedure denominate *Conosci il tuo cliente* (KYC) o *Adeguata verifica del cliente* (CDD) sono ora comuni e in molti paesi rappresentano un obbligo di legge e normativo. Tali requisiti prevedono che prima di instaurare rapporti con un nuovo cliente o effettuare un'operazione, debbano essere adottate misure appropriate per accertare chi sia il cliente e, ove pertinente, il *titolare effettivo* finale dello stesso e, ove opportuno, la controparte. Tali misure possono tradursi in controlli dell'identità relativamente semplici o possono comportare indagini più approfondite, ove le circostanze lo richiedano (ad esempio, laddove si nutrano timori in merito alle associazioni di un intermediario che abbia presentato nuovi o potenziali clienti o laddove i documenti KYC non siano stati forniti quando richiesti e senza che sia stata avanzata alcuna ragione plausibile). Le procedure KYC o CDD costituiscono un buon punto di partenza per un programma di antiriciclaggio per tutte le aziende.

Talvolta le operazioni coinvolgono altri professionisti. In alcuni casi limitati, il fatto che un acquirente o un venditore sia già stato "acquisito" da un consulente legale o contabile può indicare che sia possibile adottare un approccio più leggero in sede di procedura CDD. Si tratta di una prassi accettabile, anche se è opportuno che le aziende adottino un approccio basato sul rischio in ciascun caso (si veda la sezione 3.5). In sede di valutazione di questo rischio, le aziende e le persone fisiche dovrebbero almeno prendere in considerazione:

- l'affidabilità del professionista;
- se tale altro professionista abbia sede in una giurisdizione equivalente;
- la natura dell'operazione;
- il settore in cui il cliente opera; e
- se vi sia la necessità di condurre un'adeguata verifica rafforzata (si veda la sezione 3.6), come nei casi in cui nella proprietà o nella catena dei finanziamenti sia coinvolta una PEP.

Nel ciclo di compravendita, anche altri professionisti potrebbero essere visti come target dai riciclatori di denaro. Solo per il fatto che un legale, un finanziatore, un agente immobiliare o altro professionista sia coinvolto nella catena, non significa che il cliente o l'operazione siano legittimi. Le aziende e le persone fisiche dovrebbero tenere a mente che:

- la responsabilità finale per la valutazione del rischio del cliente e le azioni che ne conseguono da parte dell'azienda con riferimento al medesimo non può mai essere trasferita ad altri;
- gli *indicatori di allerta* di *riciclaggio di denaro* non devono essere ignorati.

Le aziende con sedi estere devono valutare come adottare un approccio comune al *riciclaggio di denaro* in tutti gli uffici. Le aziende di dimensioni più piccole o medie, che intrattengono rapporti con clienti locali e conosciuti e operano in paesi a basso rischio, hanno tuttavia minore probabilità di dover disporre di un programma di *riciclaggio di denaro* molto ampio; questo rispetto ad aziende multiservizi con sedi estere che operano in paesi a più alto rischio.

Ogni azienda trarrà beneficio dall'avvalersi di percorsi formativi idonei per il proprio personale e i propri agenti. La formazione deve essere pratica e accessibile. Anche la trasmissione di decisioni anonime in materia di *riciclaggio di denaro* è un buon modo per far sì che il personale familiarizzi con le questioni che l'azienda si trova a fronteggiare nell'attività ordinaria.

Le aziende sono tenute a documentare il loro approccio al *riciclaggio di denaro* e al *finanziamento del terrorismo*. In tutte le aziende, ad eccezione di quelle di dimensioni minori, il board/i senior manager devono essere informati, almeno una volta l'anno, in merito all'efficacia dell'approccio adottato per la gestione di tali rischi.

È importante astenersi dal segnalare problematiche con modalità di diffusione tali da condurre al reato di "divulgazione di informazioni riservate" o diversamente compromettere le parti coinvolte. Con l'espressione divulgazione di informazioni riservate si intende in senso lato comunicare o lasciare che un cliente o un terzo venga a conoscenza di una segnalazione fatta a un'autorità competente locale e/o del fatto che sia stata aperta un'indagine. Le segnalazioni dovranno essere effettuate con molta discrezione e a un numero ridotto di interlocutori. Le attività sospette di *riciclaggio di denaro* devono essere comunicate ai funzionari designati o alle persone incaricate internamente quali responsabili, che potranno dare indicazioni agli interessati su come affrontarle.

3.3 Affidamento

L'*affidamento* deve essere valutato utilizzando un approccio basato sul rischio. Nei casi in cui il cliente abbia fornito le informazioni richieste o abbia già superato i controlli previsti da un ente regolamentato in un paese in cui è registrata la sua società o nel quale avviene la transazione, quale uno studio legale o un primario istituto di credito, può essere accettabile fare affidamento sui controlli da questi effettuati sul cliente. Ciò significa l'identificazione della persona fisica sulla base delle verifiche effettuate dall'ente o dall'istituto regolamentato.

Tale approccio non sarà tuttavia accettabile nei casi in cui l'origine dei fondi sia ritenuta sospetta. Ad esempio, se un giovane che non svolge attività lavorativa, senza disponibilità liquide, effettua l'acquisto di un appartamento di lusso per importi milionari, sarà appropriato compiere ulteriori controlli sull'origine di questi fondi. In tali situazioni, la responsabilità finale per la valutazione del rischio del cliente e le azioni intraprese resterà in capo all'azienda, anche se questa si affidi ai controlli eseguiti da un terzo.

Inoltre, potrebbero essere in vigore requisiti specifici di protezione dei dati, di cui si debba tenere conto a seconda del territorio/regione, come ad esempio il lasso temporale per il quale un terzo sia tenuto o abbia diritto a detenere i dati sui quali abbia fatto affidamento.

3.4 Deroghe

Una deroga è una circostanza in cui devono essere rispettati requisiti legislativi, normativi o giudiziari specifici, che si differenziano da quelli del presente standard professionale. I membri e le aziende RICS sono tenuti a documentare per iscritto i conflitti in essere tra le leggi applicabili e il presente standard professionale, le deroghe a quest'ultimo dovute a detti conflitti e qualsiasi segnalazione o controllo supplementare implementato in conformità alle leggi applicabili.

L'obbligo di deroga al presente standard professionale ai sensi di requisiti legislativi, normativi o giudiziari prevarrà rispetto a tutti gli altri requisiti del presente standard professionale.

3.5 Approccio basato sul rischio

In sede di valutazione dei rischi, un punto di partenza utile per l'approccio basato sul rischio potrebbe essere quello di prendere in considerazione tre "domande chiave" – per conto di chi agisci, che cosa fai, perché ti viene chiesto di fare qualcosa.

Con l'approccio basato sul rischio una parte importante delle risorse viene dedicata alle aree di maggior rischio, che sono state individuate mediante la valutazione del rischio.

L'approccio basato sul rischio implica che l'uso delle risorse venga pianificato in modo proporzionato così da individuare i rischi di un'azienda. Ciò comporta la valutazione dei rischi di *corruzione*, *abuso d'ufficio*, *riciclaggio di denaro* e *finanziamento del terrorismo*, prima di formulare un piano ad hoc.

3.6 Adeguata verifica rafforzata (AVR) e Adeguata verifica semplificata (AVS)

L'*Adeguata verifica del cliente* (CDD) comporta la raccolta di evidenze standard per verificare l'identità delle diverse tipologie di clienti. Tra gli esempi sono compresi società di capitali, trust, veicoli per fini speciali, società di persone ed enti di beneficenza.

I requisiti per la conduzione di una procedura CDD variano da un paese all'altro, ma comprendono sempre i seguenti elementi:

- identificare la parte/le parti dell'operazione;
- verificare che l'identificazione sia valida; e
- condurre controlli aggiuntivi ove necessario, sulla base di taluni fattori di rischio.

Con l'espressione Adeguata verifica semplificata (AVS) si intende che non è necessario condurre una CDD completa. In una situazione che si ritenga a basso rischio di *riciclaggio di denaro*, una semplice verifica di base può essere appropriata. Le policy e le procedure interne devono stabilire (ai sensi delle leggi locali) quando possa essere applicata una AVS. Possono essere sufficienti le evidenze dello status del cliente, quali l'iscrizione al registro delle imprese locale, lo stato giuridico di una società o l'evidenza della quotazione dei titoli in una borsa valori.

Un'adeguata verifica rafforzata (AVR) sarà necessaria nelle situazioni (si veda il punto 3.9 per l'esempio delle PEP) in cui le policy o le valutazioni dell'azienda o ancora le leggi applicabili richiedano un maggiore controllo e monitoraggio per poter completare il profilo del cliente, oltre alla revisione continua del cliente o dell'operazione.

Spetta a ciascuna azienda fissare e applicare con coerenza il proprio approccio alla CDD. Alcune leggi applicabili prevedono quando si debba ricorrere a una AVS o a una AVR e devono essere rispettate. Nel Regno Unito, ad esempio, l'applicazione di una AVS non è più un'opzione automatica in tutte le situazioni e le aziende devono sempre essere attente agli indicatori di allerta che potrebbero indicare che i rischi di *riciclaggio di denaro* sono elevati e occorre procedere con un'adeguata verifica più approfondita.

I controlli circa l'origine dei fondi e l'origine del patrimonio sono inoltre strettamente collegati ai rischi di *riciclaggio di denaro* pertinenti a un'operazione o all'attività del cliente. Le aziende devono comprendere come venga finanziata un'operazione e valutare se l'entità e il senso commerciale di una data operazione soddisfino le informazioni ottenute circa il finanziamento.

Alcune situazioni giustificheranno il controllo sull'origine dei fondi, come nei casi in cui l'origine del patrimonio chiaramente non corrisponda ai fattori commerciali. Potranno pertanto rendersi necessarie informazioni quali estratti conto bancari, atti fiduciari o evidenze di pagamenti di premi, che a loro volta condurranno ad ulteriori indagini.

Il fatto di sapere quando effettuare controlli sull'origine dei fondi e comprendere profondamente il profilo patrimoniale e finanziario di un cliente dipende dall'esperienza e deve generalmente essere descritto nelle procedure aziendali e nei percorsi formativi.

I professionisti devono inoltre essere attenti alla necessità di aggiornare di tanto in tanto la CDD dei rispettivi clienti e sono tenuti a predisporre una policy in merito. La revisione delle informazioni con cadenza triennale può ritenersi appropriata in molte situazioni. Possono insorgere rischi quando un cliente a basso rischio sia stato acquisito per una data questione e rimanga "nel sistema" per un'operazione molto più rischiosa, ma successiva. In questi casi il rischio è che l'azienda non aggiorni il profilo di rischio del cliente portandolo al livello superiore in quanto questi ha già superato controlli interni di soglia inferiore. In caso di rapporti d'affari duraturi con un cliente, sarebbe una best practice richiedere la documentazione identificativa aggiornata all'inizio di ciascuna nuova operazione oppure ad intervalli periodici e frequenti (proprio come accade nelle operazioni commerciali).

3.7 Tutore della compliance e dell'etica

La nomina di un tutore della compliance e dell'etica è un modo potenzialmente molto efficace per supportare i sistemi integrati che contribuiscono a individuare e contrastare il *riciclaggio di denaro* e il *finanziamento del terrorismo*, la *corruzione* e l'*abuso d'ufficio*. In genere questo incarico viene assegnato a un alto dirigente con una buona esperienza nell'attività aziendale e grande visibilità in un reparto o ufficio. Le aziende soggette a limiti per effetto delle rispettive dimensioni e/o risorse potrebbero non essere in grado di assegnare tale funzione a un alto dirigente, ma dovrebbero adottare misure appropriate.

Questi tutori possono disporre di una panoramica generale delle persone responsabili della CDD e dell'etica dell'azienda. Possono contribuire a promuovere le good practice e godono di una posizione di privilegio per quanto riguarda la conoscenza dei rischi ordinari che insorgono, essendo pertanto in grado di informare gli alti dirigenti di eventuali nuovi rischi e fornire raccomandazioni pratiche in merito ai controlli idonei. I tutori possono anche gestire le indagini interne, ove necessarie, e in tal caso rappresentano una risorsa preziosa per i consulenti legali o i professionisti del ramo della compliance interni ed esterni.

Per le aziende con una base di risorse più ampia, probabilmente vi è già un tutore responsabile della CDD, pertanto sarà sufficiente formalizzare questo ruolo nell'ambito dell'approccio alla governance per il *riciclaggio di denaro*. Le aziende soggette a limiti di risorse potrebbero individuare in questi tutori un modo efficace per fronteggiare una maggiore domanda.

3.8 Codice di condotta

Un codice di condotta è un documento formale, generalmente breve, che sancisce l'impegno dell'azienda rispetto alla buona etica e quanto ci si attende dai collaboratori dell'azienda. Tale documento può illustrare la condotta corretta in talune circostanze e indicare i referenti da contattare in caso di bisogno.

Come accade per diverse delle misure suggerite, il fatto di disporre di un codice di condotta scritto dipenderà dalla dimensione, dalla complessità e dall'ubicazione di ciascuna azienda. Tale documento potrebbe non essere necessario per un'azienda con uno o due uffici di meno di 25 dipendenti in totale. Le aziende di dimensioni maggiori sono tenute a decidere autonomamente se valga o meno la pena predisporre un codice di condotta.

3.9 Persone politicamente esposte (PEP)

Le PEP rappresentano un rischio elevato dal punto di vista del *riciclaggio di denaro* e dell'*abuso d'ufficio* in quanto ricoprono posizioni di influenza - in effetti, molte giurisdizioni legiferano in materia. È opportuno sottolineare che per il semplice fatto che una persona fisica sia stata identificata come PEP non significa che un'azienda debba automaticamente rifiutare di effettuare operazioni con la stessa o trattare le rispettive operazioni con sospetto.

L'approccio corretto nel relazionarsi con una PEP consiste nel disporre di una policy che consenta di profilare tale PEP su una base di rischio. Molte aziende dispongono di sistemi di ricerca automatizzati per tutti i nuovi clienti (e fornitori e agenti nei paesi ad alto rischio), che evidenziano se una data persona sia una PEP. Le aziende di dimensioni più piccole possono effettuare ricerche sulla base di criteri di rischio prefissati e chiedere direttamente ai clienti se siano PEP.

Laddove si stabilisca che un cliente, o potenziale cliente, sia una PEP, questo dovrebbe condurre all'esecuzione di una AVR sul cliente. Nell'ambito di questo processo, occorrerà effettuare una valutazione più approfondita della tipologia di operazione e potenzialmente dell'origine dei fondi da utilizzare. Le decisioni adottate relativamente a una PEP devono essere documentate. Gli alti dirigenti devono essere coinvolti nel processo decisionale volto a stabilire se procedere con un'operazione che coinvolga una PEP come parte o se essa stia concedendo un finanziamento a terzi (ad esempio, un genitore che finanzia l'acquisto della casa per il figlio).

Nelle contrattazioni con le società di capitali o altri soggetti giuridici, si applicheranno gli stessi processi nel caso in cui il *titolare effettivo* sia una PEP.

3.10 Titolarità effettiva

Nella maggior parte delle entità (società di persone, società di capitali e trust), il *titolare effettivo* sarà la persona che detiene o controlla in ultima istanza una percentuale minima definita per legge di azioni o diritti di voto di tale entità. Alcune leggi fissano questo valore al 25 percento o quota superiore, altre al 10 percento o quota superiore. Nel caso di trust, ci si riferisce a una quota di partecipazione, in percentuale minima definita, del capitale del patrimonio del trust o, laddove non vi sia alcun beneficiario specifico, alla persona che controlla il trust o nel cui interesse principale esso sia stato costituito.

Il *titolare effettivo* di un'organizzazione del cliente può essere individuato richiedendo la trasmissione di documenti utili, quali un recente Atto costitutivo o la Dichiarazione dei redditi di una società, o la conferma scritta di un consulente legale che dichiari chi siano i *titolari effettivi* del trust.

3.11 Whistleblowing

A seconda delle dimensioni, potrebbe essere appropriato per le aziende regolamentate da RICS disporre di una policy in materia di whistleblowing che definisca quando e come i dipendenti debbano segnalare le loro preoccupazioni e come saranno trattate tali segnalazioni. Nel caso di PMI, il fatto di disporre di una policy in materia di whistleblowing potrebbe rappresentare un costo eccessivo e pertanto non è richiesto. Per le imprese di maggiori dimensioni risulterà invece complicato spiegare quali siano le ragioni per le quali non abbiano adottato una policy simile. Ove pertinente, questa policy dovrebbe fornire linee guida per coloro che intendano effettuare segnalazioni delle violazioni ma che si trovino, per ragioni locali stringenti (quali guerre, instabilità politica e disastri naturali), a non poter procedere con i soliti canali, indicando canali sicuri alternativi per la segnalazione.

Riferimenti

Gruppo di Azione Finanziaria Internazionale (GAFI). *Money laundering FAQ* (FAQ sul riciclaggio di denaro). Indirizzo: **www.fatf-gafi.org/faq/moneylaundering/** (accesso 24.10.18).

RICS (2017). *Conflitti di interesse, globali*, prima edizione. Londra: RICS.

RICS (2007). *Codice deontologico RICS per le Aziende*, versione 6, in vigore dal 25 aprile 2017. Londra: RICS.

RICS (2007). *Codice deontologico RICS per i Membri*, versione 6, in vigore dal 1° gennaio 2013. Londra: RICS.

Transparency International (2017). *Corruption Perceptions Index* (indice di percezione della corruzione). Indirizzo: **https://www.transparency.org/research/cpi/overview** (accesso 24.10.18).

Approfondimenti

Il presente materiale non comprende le importanti linee guida locali emanate dai governi nazionali, dalle autorità di vigilanza e dai regolatori in considerazione del livello globale del presente standard professionale.

Deloitte (2015). *Building world class ethics and compliance programs* (costruire programmi di etica e compliance di livello mondiale). Indirizzo: **https://www2.deloitte.com/content/dam/Deloitte/no/Documents/risk/Building-world-class-ethics-and-compliance-programs.pdf** (accesso 24.10.18).

GAFI (2018). *Concealment of beneficial ownership* (occultamento della titolarità effettiva). Indirizzo: **http://www.fatf-gafi.org/publications/methodsandtrends/documents/concealment-beneficial-ownership.html** (accesso 24.10.18).

GAFI (2018). *Consolidated assessment ratings* (rating consolidati di valutazione). Indirizzo: http://www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html (accesso 24.10.18).

GAFI (2018). *Professional money laundering* (riciclaggio di denaro professionale). Indirizzo: **http://www.fatf-gafi.org/publications/methodsandtrends/documents/professional-money-laundering.html** (accesso 24.10.18).

ISO 37001: 2016. *Sistemi di gestione per la prevenzione della corruzione - Requisiti e linee guida per l'uso*. Ginevra: ISO.

OCSE (2018). *Guida dell'OCSE sul dovere di diligenza per la condotta d'impresa responsabile*. Indirizzo: **https://www.oecd.org/investment/due-diligence-guidance-for-responsible-business-conduct.htm** (accesso 24.10.18).

Transparency International (2017). *FAQs on corruption* (FAQ sulla corruzione). Indirizzo: **https://www.transparency.org/whoweare/organisation/faqs_on_corruption** (accesso 24.10.18).

Banca Mondiale (2009). *Combating money laundering and the financing of Terrorism – A comprehensive training guide* (lotta al riciclaggio di denaro e al finanziamento del terrorismo - una guida completa). Indirizzo: **http://siteresources.worldbank.org/FINANCIALSECTOR/Resources/CombattingMLandTF.pdf** (accesso 24.10.18).

RICS (2017). *Codice deontologico*. **https://www.rics.org/uk/upholding-professional-standards/standards-of-conduct/rules-of-conduct/**

RICS (2017). *Conflitti di interesse*. **https://www.rics.org/uk/upholding-professional-standards/standards-of-conduct/conflicts-of-interest/**

Appendici

1 I modelli forniti sono pensati per essere utili alle aziende regolamentate da RICS e ai membri RICS, ma non costituiscono formali linee guida RICS. I modelli non sono pensati per essere un riferimento completo, né si dovrebbe interpretarli come tali, a tutte le azioni necessarie e/o appropriate.

2 L'affidamento su questi modelli è a proprio rischio.

3 Il grado di dettaglio dipenderà ampiamente dal tipo e dalla dimensione dell'azienda in questione e, a tale scopo, questo schema dovrebbe essere usato in modo flessibile nell'ambito di ciascuna azienda.

4 Alcuni aspetti del modello potrebbero non applicarsi o essere pertinenti per una data azienda.

5 Compete all'azienda regolamentata da RICS o al membro RICS stabilire se siano appropriati ulteriori dettagli e controlli oltre a quelli indicati in questi modelli.

Appendice A

Modello del modulo di due diligence del cliente

A: [soggetti interessati dai controlli di due diligence]

[Per le persone fisiche]

La preghiamo di fornire, per ciascuna persona fisica, un documento identificativo in corso di validità con foto, ad esempio un passaporto o una patente di guida con evidenza recente dell'indirizzo.

[Per le entità diverse dalle persone fisiche (ad esempio, società di capitali, società di persone o trust)]

La preghiamo di fornire un identificativo unico per l'entità, ad esempio il numero di registrazione della società o il numero di registrazione SSIP.

La preghiamo di fornire i documenti dai quali si evinca che Lei è autorizzato ad agire per conto di questa entità.

La preghiamo di fornire l'indirizzo della sua sede legale e, se diverso, della sua sede principale di attività.

Qualora Lei o la sua società controllante/capogruppo fosse quotata su una borsa valori, la preghiamo di fornirne le evidenze. In caso contrario, la preghiamo di fornire un organigramma indicante la partecipazione attuale, la struttura di controllo (ivi comprese tutte le entità che si situano tra il cliente e il titolare effettivo finale) e l'identità di qualsiasi persona fisica/entità che detenga più di una data percentuale [ad esempio, il 25%] dei suoi diritti di voto e/o diritti di controllo.

La preghiamo di fornire un estratto in corso di validità dei suoi documenti di registrazione, ad esempio della dichiarazione dei redditi, dell'atto costitutivo, del certificato di vigenza, dello statuto societario, una copia dei libri contabili o dell'atto costitutivo del trust.

Appendice B

Bozza dei controlli in materia di compliance in capo all'azienda

Coloro a cui spetta il compito di effettuare un'adeguata verifica del cliente in seno all'azienda dovrebbero eseguire i seguenti controlli al fine di verificare le informazioni fornite dal potenziale cliente nel modulo di due diligence:

- incontrare personalmente il potenziale cliente;
- verificare la copia fisica dei documenti identificativi del potenziale cliente o una copia degli stessi autenticata da un consulente legale appropriato;
- verificare la validità dei documenti forniti da un'entità diversa da una persona fisica;
- controllare se il potenziale cliente (o il rispettivo titolare effettivo finale) sia una Persona politicamente esposta (PEP) o un parente stretto o un familiare di una PEP;
- controllare se il potenziale cliente (o il rispettivo titolare effettivo finale) sia soggetto a sanzioni pertinenti che proibiscano all'azienda di instaurare un rapporto d'affari con lo stesso;
- accertare le finalità e la natura prevista del potenziale rapporto d'affari e dell'operazione;
- controllare dove abbia sede il potenziale cliente e, in caso di sede principale all'estero, se si tratti di un paese terzo ad alto rischio;
- controllare quali siano il settore aziendale e l'attività principali del potenziale cliente.

Sulla base di questi controlli, accertare se si debba applicare al potenziale cliente un'adeguata verifica rafforzata (AVR).

Bozza della richiesta di informazioni relativa alla titolarità effettiva

A: [strutture societarie complesse o offshore la cui titolarità effettiva sia oggetto della richiesta di informazioni]

[La legislazione pertinente] ci obbliga ad accertarci dei titolari effettivi delle parti di un'operazione, ivi compresi coloro che agiscono in veste di società di capitali, società di persone, trust o altra entità (o una combinazione di queste). In termini pratici con l'espressione titolare effettivo si intende stabilire chi sia la persona o le persone che detengono oltre una data percentuale [ad esempio, il 25%] di un'entità, nonché coloro che gestiscono o controllano l'entità se diversi dai titolari.

Nel caso in cui non fossimo in grado di effettuare prontamente le indagini (per stabilire la titolarità effettiva) per mezzo di database nazionali di ricerca e in qualsiasi delle seguenti circostanze:

- la società di capitali è registrata all'estero;
- è coinvolto un trust;
- è coinvolto qualsiasi tipo di società di persone;

le richiederemo di fornirci i documenti necessari per comprovare la sua struttura e, in ultima istanza, chi siano i suoi titolari effettivi. Comprendendo che la terminologia potrebbe differire, le seguenti tipologie di documenti potrebbero essere utili:

- **Società di capitali:** atto costitutivo, dichiarazione dei redditi o documento analogo recente (che specifichi in dettaglio l'identità degli azionisti) che ci consenta di identificare i singoli azionisti alla soglia richiesta (ad esempio, il 25%) o superiore delle sue azioni/dei suoi diritti di voto.
- **Trust:** conferma scritta fornita da un consulente legale (che potrebbe essere un trustee) o da un trustee che dichiari l'identità dei titolari effettivi del trust; in genere questi saranno i beneficiari o i trustee o, laddove non siano ancora noti o non siano persone fisiche specifiche, i trustee si riterranno generalmente essere i titolari effettivi.
- **Società di persone:** atto costitutivo della società di persone, ultimo bilancio, o lettera di conferma della titolarità effettiva dell'avvocato o del consulente contabile.

Questi documenti sono altresì richiesti per ciascun livello della struttura "sottostante" ai titolari effettivi.

Checklist antiriciclaggio

Numero di pratica: ..... **Nome del cliente:** .....

Nome del bene: .....

Documento comprovante la proprietà: Catasto nazionale: ☐ Copia della locazione: ☐

Altro: .....

Lettera di autorizzazione ad agire per conto del cliente (se richiesta):

Livello di due diligence (KYC): Normale: ☐ Semplificata: ☐ Rafforzata: ☐

Se semplificata o rafforzata, spiegarne le ragioni:

.....

.....

.....

Titolari effettivi (persone)

Nome: ..... Doc. Identità: ☐ Doc. attestante indirizzo: ☐ Controllo on-line: ☐

Nome: ..... Doc. Identità: ☐ Doc. attestante indirizzo: ☐ Controllo on-line: ☐

Nome: ..... Doc. Identità: ☐ Doc. attestante indirizzo: ☐ Controllo on-line: ☐

Struttura della proprietà (inserire la denominazione delle entità, la % detenuta e la gerarchia):

.....

.....

CERTIFICO

di aver verificato l'identità del cliente e di aver visionato i documenti originali e posso confermare che qualsiasi fotografia associata al cliente raffigura con buona probabilità il medesimo E/O che tutte le copie autenticate sono firmate. I miei controlli AML sono stati completati in conformità alla Policy e alle Procedure AML della società e riconosco di essere responsabile della relativa completezza e correttezza.

Nome del professionista incaricato: ..... **Firma:** .....

Ufficio: ..... **Data:** .....

Appendice C

Modello della lettera di affidamento

Da: [inserire il nome e l'indirizzo della persona su cui si fa affidamento]

A:

Data:

Gentile [nome]

Con la presente, [io/noi] confermo/confermiamo di aver ricevuto la sua lettera datata [inserire la data] relativa alla sua richiesta di fare affidamento sui [miei/nostri] controlli di due diligence del cliente con riferimento a [cliente] in conformità alla [legislazione pertinente].

In risposta alla sua richiesta:

[confermo/confermiamo] di essere un [agente immobiliare] secondo la definizione fornita dalla [legislazione locale];

[confermo/confermiamo] di aver applicato i provvedimenti di due diligence del cliente in relazione a [cliente] come previsto dalla [legislazione pertinente];

[acconsento/acconsentiamo] a che Lei faccia affidamento, per le finalità esposte nella sua lettera e in via limitativa, sui provvedimenti di due diligence del cliente previsti dalla [legislazione pertinente];

[confermo/confermiamo] di conservare la documentazione relativa ai controlli di due diligence del cliente da [me/noi] effettuati come indicato per il periodo previsto dalla [legislazione pertinente];

[accetto/accettiamo] di mettere a sua disposizione, non appena possibile e dietro sua richiesta, qualsiasi informazione e copia dei dati identificativi e di verifica relativi a [cliente] [e qualsiasi titolare effettivo] da [me/noi] ottenuti in sede di applicazione dei provvedimenti di due diligence del cliente;

[confermo/confermiamo] che il [mio/nostro] organismo di vigilanza ai fini del riciclaggio di denaro è/sono [inserire la denominazione, ad esempio, UIF – Unità di Informazione Finanziaria, istituita presso la Banca d'Italia] o che ci atteniamo a standard equivalenti a quelli vigenti nei Paesi del SEE.

Lei accetta e garantisce che le informazioni da noi fornitele in conformità alla presente lettera e alla [legislazione pertinente] saranno utilizzate ai soli fini dei suoi obblighi ai sensi della [legislazione pertinente locale dell'affidatario] e non per qualsivoglia altra finalità e che i dati personali o sensibili che le abbiamo fornito rispetto a qualsiasi cliente o persona fisica o entità in conformità alla presente lettera saranno trattati di conseguenza. Lei conferma altresì di attenersi a tutte le leggi sulla protezione dei dati pertinenti di volta in volta in vigore all'atto del trattamento e della gestione dei dati forniti.

Con l'accettazione della presente lettera, Lei conferma la nostra non responsabilità nei suoi confronti o nei confronti di terzi con riferimento alle conferme ivi contenute e per null'altro. La conformità alla legislazione pertinente è e rimane di sua esclusiva responsabilità.

[Nome della persona sulla quale si fa affidamento e posizione in seno all'azienda]

Fiducia attraverso gli standard professionali

RICS sviluppa e regolamenta le più importanti qualifiche professionali e gli standard riconosciuti negli ambiti della valutazione, dello sviluppo e della gestione del real estate, del territorio, delle costruzioni e delle infrastrutture. Il nostro nome è sinonimo di qualità: promuovendo l'utilizzo coerente degli standard assicuriamo la trasparenza del mercato e la crescita dei settori in cui operiamo.

America

America Latina
ricsamericalatina@rics.org

Nord America
ricsamericas@rics.org

APAC

Australasia
australasia@rics.org

Cina (Hong Kong)
ricshk@rics.org

Cina (Shanghai)
ricschina@rics.org

Giappone
ricsjapan@rics.org

Asia Meridionale
ricsindia@rics.org

Sud-est asiatico
sea@rics.org

EMEA

Africa
ricsafrica@rics.org

Europa
ricseurope@rics.org

Irlanda
ricsireland@rics.org

Medio Oriente
ricsmiddleeast@rics.org

Regno Unito (RICS HQ)
contactrics@rics.org

rics.org

ITALIAN/AUGUST 2019/LANDOOR/PRJ0540-19/CANOPY/PS