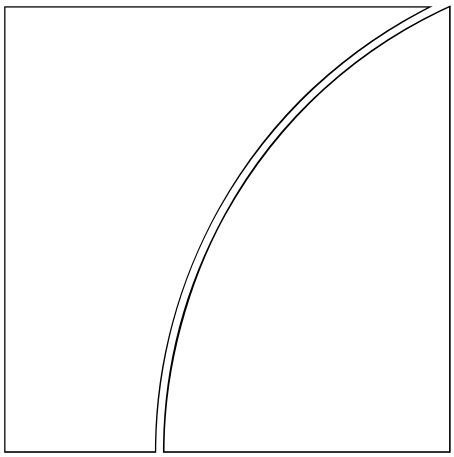
Comitato di Basilea
per la vigilanza bancaria



Dovere di diligenza delle banche nell'identificazione della clientela

Ottobre 2001

BANCA DEI REGOLAMENTI INTERNAZIONALI

Gruppo di lavoro sull'attività bancaria transfrontaliera

Co-Presidenti:

Charles Freeland, Vice Segretario Generale del Comitato di Basilea per la vigilanza bancaria

Colin Powell, Presidente del Gruppo Offshore di autorità di vigilanza bancaria e Presidente della Jersey Financial Services Commission

Bermuda Monetary Authority	D. Munro Sutherland
Cayman Islands Monetary Authority	John Bourbon Anna McLean
Banque de France/Commission Bancaire	Laurent Ettori
Bundesamt für Bankenaufsicht, Germania	Jochen Sanio Peter Kruschel
Guernsey Financial Services Commission	Peter G. Crook (fino all'aprile 2001) Philip Marr (dall'aprile 2001)
Banca d'Italia	Giuseppe Godano
Financial Services Agency, Giappone	Kiyotaka Sasaki (fino al luglio 2001) Hisashi Ono (dal luglio 2001)
Commission de Surveillance du Secteur Financier, Lussemburgo	Romain Strock
Monetary Authority of Singapore	Foo-Yap Siew Hong Teo Lay Har
Commissione federale per le banche, Svizzera	Daniel Zuberbühler Dina Balleyguier
Financial Services Authority, Regno Unito	Richard Chalmers
Board of Governors of the Federal Reserve System	William Ryback
Federal Reserve Bank of New York	Nancy Bercovici
Office of the Comptroller of the Currency	Jose Tuya Tanya Smith
Segretariato	Andrew Khoo

Indice

Dovere di diligenza delle banche nell'identificazione della clientela

I. Introduzione

1. Le autorità di vigilanza di tutto il mondo sono sempre più consapevoli dell'importanza di assicurare che le banche di propria pertinenza pongano in atto adeguati controlli e procedure per conoscere i clienti con cui operano. L'esercizio della dovuta diligenza nei confronti della clientela esistente e di nuova acquisizione costituisce un elemento essenziale di tali controlli, in assenza del quale le banche possono esporsi a rischi di reputazione, operativi, legali e di concentrazione, e conseguentemente incorrere in costi finanziari considerevoli.

2. Analizzando i risultati di un'inchiesta interna del 1999 sull'attività bancaria transfrontaliera, il Comitato di Basilea ha rilevato come in numerosi paesi vi siano carenze nelle politiche delle banche per l'identificazione dei clienti ("know-your-customer", KYC). Giudicate in un'ottica di vigilanza, tali politiche mostrano gravi lacune in alcuni paesi, mentre in altri appaiono del tutto assenti. Anche nell'ambito dei paesi con mercati finanziari evoluti gli standard non sono uniformi. Pertanto, il Comitato ha chiesto al Gruppo di lavoro sull'attività bancaria transfrontaliera[1] di esaminare le procedure KYC attualmente in uso e di elaborare raccomandazioni applicabili alle banche di tutti i paesi. Il rapporto che ne è scaturito è stato pubblicato a fini consultivi nel gennaio 2001. Dopo un'attenta valutazione dei commenti ricevuti, il Gruppo di lavoro ha redatto un nuovo documento riveduto che il Comitato distribuisce oggi su scala mondiale, confidando che lo schema in esso proposto venga assunto come riferimento dalle autorità di vigilanza nella definizione di standard nazionali e dalle banche nella formulazione dei propri programmi. È importante riconoscere che in talune giurisdizioni le pratiche di vigilanza soddisfano già, o vanno addirittura oltre, i requisiti stabiliti nel presente documento e potrebbero quindi non richiedere alcuna modifica.

3. Le procedure KYC sono intimamente collegate alla lotta contro il riciclaggio dei fondi di provenienza illecita, che è essenzialmente di pertinenza della Financial Action Task Force (FATF)[2]. Non è intenzione del Comitato duplicare le iniziative della FATF. Il suo interesse si colloca infatti in una più ampia prospettiva prudenziale. L'applicazione di corrette politiche e procedure KYC è essenziale al fine di salvaguardare la sicurezza e la solidità delle banche, nonché l'integrità del sistema bancario. Il Comitato di Basilea e il Gruppo offshore di autorità di vigilanza bancaria (Gruppo offshore) continueranno a sostenere fermamente l'adozione e l'applicazione pratica delle raccomandazioni FATF, specie quelle riguardanti le banche, ed è loro intendimento che gli standard stabiliti in questo documento siano coerenti con tali raccomandazioni. Il Comitato di Basilea e il Gruppo offshore considereranno inoltre l'adozione di eventuali requisiti più stringenti introdotti dalla FATF in sede di revisione delle sue 40 Raccomandazioni. Di conseguenza, il Gruppo di lavoro rimarrà in stretto contatto con la FATF per seguire attentamente le sue deliberazioni.

4. L'approccio del Comitato di Basilea al KYC si pone in un'ottica di vigilanza più ampia, non incentrata unicamente sulla lotta al riciclaggio di proventi illeciti. L'applicazione di corrette procedure KYC va riguardata come elemento cruciale di un'efficace gestione dei rischi bancari. Le salvaguardie in questo ambito non concernono soltanto l'apertura dei conti e la tenuta della documentazione, ma implicano anche la formulazione di una politica per l'accettazione della clientela e di un programma

---

[1] Gruppo congiunto formato da membri del Comitato di Basilea e del Gruppo offshore di autorità di vigilanza bancaria.

[2] La FATF (nota anche come "Gruppo di azione finanziaria", GAFI) è un ente intergovernativo, costituito da 29 paesi membri e due organismi regionali, che elabora e promuove, a livello sia nazionale che internazionale, direttive per combattere il riciclaggio di denaro. Essa opera in stretta collaborazione con altri organismi internazionali attivi in questo campo, quali l'Office for Drug Control and Crime Prevention delle Nazioni Unite, il Consiglio d'Europa, l'Asia-Pacific Group on Money Laundering e la Caribbean Financial Action Task Force. La FATF definisce il riciclaggio di denaro come il trattamento dei proventi di attività delittuose allo scopo di dissimularne l'origine illegale.

articolato per la sua identificazione, che preveda una più scrupolosa diligenza nei riguardi dei conti a maggiore rischio, nonché il loro monitoraggio attivo al fine di rilevare eventuali attività sospette.

5. L'interesse del Comitato di Basilea per una corretta prassi KYC origina dalla sua preoccupazione per l'integrità del mercato ed è stato accentuato dalle perdite dirette e indirette subite da talune banche in seguito alla loro mancanza di diligenza nell'applicare adeguate procedure. Probabilmente tali perdite avrebbero potuto essere evitate, e i danni in termini di reputazione notevolmente ridotti, se le istituzioni in questione avessero adottato efficaci programmi KYC.

6. Il presente documento rafforza i principi stabiliti in precedenti pubblicazioni del Comitato, fornendo orientamenti più precisi riguardo agli elementi essenziali delle procedure KYC e alla loro applicazione pratica. Nell'elaborare le linee guida il Gruppo di lavoro si è basato sulle pratiche vigenti nei paesi membri e ha tenuto conto dell'evoluzione in campo prudenziale. Gli elementi essenziali presentati in questo documento vanno intesi come requisiti minimi applicabili a tutte le banche su scala mondiale. Tali requisiti potranno essere integrati e/o rafforzati mediante prescrizioni addizionali commisurate ai rischi presenti in determinate istituzioni e nel sistema bancario di singoli paesi. Ad esempio, un'accresciuta diligenza è richiesta per i conti a più alto rischio o per le banche che mirano specificatamente ad attirare clienti dotati di patrimoni di ingente ammontare. In varie sezioni del documento sono contenute raccomandazioni per l'adozione, ove applicabile, di criteri di diligenza più stringenti nelle aree di maggiore rischio all'interno di una banca.

7. La necessità di rigorosi standard di diligenza riguardo alla clientela non concerne soltanto le banche. Il Comitato di Basilea è del parere che raccomandazioni analoghe vadano formulate anche per le istituzioni finanziarie non bancarie e per gli intermediari professionisti che operano in ambito finanziario, come avvocati e commercialisti.

II. Importanza dei requisiti KYC per le autorità di vigilanza e le banche

8. La FATF e altri gruppi internazionali hanno lavorato intensamente sulla problematica KYC, e le 40 Raccomandazioni emanate dalla FATF per combattere il riciclaggio di denaro[3] trovano riconoscimento e attuazione su scala internazionale. Non è intenzione del presente documento duplicare tale lavoro.

9. Al tempo stesso, l'applicazione di rigorose procedure KYC ha particolare rilevanza ai fini della sicurezza e solidità delle banche, in quanto essa:

- contribuisce a proteggere la reputazione delle istituzioni e l'integrità dei sistemi bancari, limitando il pericolo che gli enti creditizi diventino veicoli o vittime di crimini finanziari e subiscano conseguenti danni di immagine;
- è parte essenziale di una sana gestione del rischio (fornendo tra l'altro la base per individuare, limitare e controllare le esposizioni al rischio insite negli elementi attivi e passivi del patrimonio, ivi compresi gli averi ricevuti in amministrazione).

10. L'inadeguatezza o l'assenza di standard KYC può esporre le banche a gravi rischi nei confronti della clientela e delle controparti, e in particolare a ***rischi di reputazione, operativi, legali*** e ***di concentrazione***. Va rilevato che tutti questi rischi sono correlati. Nondimeno, ognuno di essi può comportare ingenti oneri finanziari (causati ad esempio da ritiro di depositi, revoca di linee creditizie interbancarie, richiesta di danni, costi di investigazione, misure cautelative e sequestrative a carico di cespiti patrimoniali, perdite su crediti), nonché costringere il management a dedicare tempo ed energie alla risoluzione dei problemi che ne conseguono.

11. Il ***rischio di reputazione*** costituisce una grave minaccia per le banche, poiché la natura stessa della loro attività presuppone il mantenimento della fiducia dei depositanti, dei creditori e del mercato in generale. Il rischio di reputazione può definirsi come la possibilità che la diffusione di notizie negative, siano esse veritiere o meno, concernenti le modalità di gestione o le connessioni di una banca intacchino la fiducia nella sua integrità. Le banche sono particolarmente esposte a questo

[3] Si vedano le Raccomandazioni 10-19 della FATF, riportate nell'Allegato 2.

tipo di rischio in quanto possono facilmente diventare strumento o vittima di attività illecite compiute da propri clienti. Esse devono proteggersi esercitando una vigilanza costante mediante l'applicazione di rigorose procedure KYC. Particolari rischi di reputazione possono derivare dalle attività detenute in amministrazione o su base fiduciaria.

12. Il ***rischio operativo*** è definibile come il rischio di perdite dirette o indirette derivanti da disfunzioni a livello di procedure, personale e sistemi interni, oppure da eventi esogeni. Nel contesto dell'identificazione della clientela il rischio operativo è per lo più collegato a deficienze nell'attuazione dei programmi, all'inefficacia delle procedure di controllo e al mancato esercizio della dovuta diligenza. La percezione da parte del pubblico che una banca non sia capace di gestire in modo efficace il proprio rischio operativo può compromettere o influenzare negativamente l'attività dell'istituzione.

13. Il ***rischio legale*** è il rischio che azioni legali, sentenze avverse o contratti rivelatisi giuridicamente inefficaci possano pregiudicare o perturbare l'operatività o le condizioni di una banca. Le banche possono essere chiamate in giudizio per l'inosservanza di requisiti cogenti in materia di identificazione dei clienti o per il mancato esercizio della dovuta diligenza e, in conseguenza di ciò, subire multe, procedimenti penali e sanzioni speciali inflitte dalle autorità di vigilanza. Di fatto, per una banca coinvolta in un procedimento giudiziario le implicazioni finanziarie negative possono andare ben oltre i semplici costi legali. Le banche sono nell'impossibilità di tutelarsi efficacemente contro tali rischi legali se non esercitano la dovuta diligenza nell'identificare i propri clienti e nel conoscere le attività che questi svolgono.

14. Sul piano prudenziale i timori circa il ***rischio di concentrazione*** riguardano essenzialmente il lato degli impieghi bancari. Di regola, le autorità di vigilanza non soltanto richiedono alle banche di disporre di sistemi informativi che consentano loro di individuare le concentrazioni dei fidi, ma solitamente pongono anche limiti all'esposizione verso singoli mutuatari o gruppi di mutuatari collegati. Se una banca non conosce esattamente l'identità dei suoi affidati e le loro connessioni con altri clienti, essa non sarà in grado di misurare il rischio di concentrazione. Ciò assume particolare rilevanza nel contesto dei prestiti a entità consociate e a soggetti collegati.

15. Dal lato del passivo il rischio di concentrazione è intimamente correlato al rischio di finanziamento, e in particolare al rischio di un imprevisto ritiro anticipato di fondi da parte di grandi depositanti, con effetti potenzialmente deleteri per la liquidità della banca. Il rischio di finanziamento tende a essere più elevato nel caso degli istituti di dimensioni modeste o meno attivi sui mercati all'ingrosso. Per poter analizzare le concentrazioni dal lato della provvista è necessaria una buona conoscenza delle caratteristiche dei depositanti, intendendo con ciò non soltanto l'identità, ma anche la misura in cui le loro azioni possono essere interrelate. È essenziale che nelle banche di piccole dimensioni i responsabili della gestione del passivo non si limitino a conoscere i maggiori depositanti, ma mantengano con essi rapporti assidui, onde evitare di perdere la disponibilità dei loro fondi nei momenti critici.

16. Non di rado i clienti hanno più conti nella stessa banca, ma presso sportelli situati in paesi diversi. Al fine di gestire efficacemente i rischi di reputazione, di conformità e legali che possono risultare dall'esistenza di tali conti, le banche dovrebbero essere in grado di aggregarne e monitorarne le giacenze e i movimenti su una base pienamente consolidata a livello mondiale, a prescindere dalla forma tecnica (strumenti in bilancio o fuori bilancio, fondi in amministrazione o depositi fiduciari) in cui sono detenuti gli averi.

17. Il Comitato di Basilea e il Gruppo offshore di autorità di vigilanza bancaria sono fermamente convinti che l'applicazione di rigorose procedure KYC debba essere parte integrante dei sistemi di gestione del rischio e di controllo interno di tutte le banche del mondo. Le autorità di vigilanza nazionali sono tenute ad assicurare che le istituzioni di propria pertinenza attuino requisiti minimi di diligenza e controlli interni idonei a fornire una conoscenza adeguata dei propri clienti. I codici di comportamento volontari[4] emanati da organismi o associazioni di categoria possono essere di grande utilità come complemento delle direttive regolamentari, fornendo alle banche indicazioni pratiche in ordine a specifiche questioni operative. Essi non possono tuttavia sostituirsi alle prescrizioni ufficiali.

---

[4] Un esempio di codice di questo genere è fornito dalle "Global anti-money-laundering guidelines for Private Banking" (note anche come "principi Wolfsberg"), redatte nell'ottobre 2000 da dodici grandi banche con una importante operatività nel settore del private banking.

III. Elementi essenziali dei requisiti KYC

18. Le linee guida del Comitato di Basilea in merito alle politiche KYC sono contenute nei seguenti tre documenti, che riflettono l'evoluzione dell'approccio prudenziale nel corso del tempo. Il documento *Prevenzione dell'utilizzo del sistema bancario per il riciclaggio di fondi di provenienza illecita*, pubblicato nel 1988, enuncia i principi etici basilari e incoraggia le banche a porre in essere efficaci procedure per identificare la clientela, a rifiutare l'esecuzione di transazioni sospette e a collaborare con le autorità giudiziarie e di polizia. I *Principi fondamentali per un'efficace vigilanza bancaria* del 1997 stabiliscono, nel quadro di una più ampia analisi dei controlli interni, che le banche dovrebbero adottare politiche, prassi e procedure adeguate, fra cui rigorose regole per l'identificazione della clientela; in particolare, le autorità di vigilanza dovrebbero incoraggiare l'adozione delle raccomandazioni della FATF. Esse riguardano l'identificazione dei clienti e la conservazione dei relativi documenti, un'accresciuta diligenza da parte delle istituzioni finanziarie nell'individuare e segnalare le operazioni sospette, nonché le misure da applicare nei rapporti con i paesi in cui vigono prescrizioni inadeguate contro il riciclaggio di capitali illeciti. Il documento *Metodologia dei Principi fondamentali per un'efficace vigilanza bancaria* del 1999 elabora ulteriormente tali Principi enunciando una serie di criteri essenziali e integrativi (nell'Allegato 1 sono riportati i passaggi rilevanti tratti dai due documenti).

19. A ogni banca dovrebbe essere richiesto di disporre di "adeguate politiche, prassi e procedure per promuovere un elevato standard etico e professionale e per impedire che la banca si presti, con o senza intenzionalità, a essere utilizzata da soggetti criminali"[5]. Nei programmi KYC delle banche andrebbero incorporati determinati elementi essenziali. Questi inizieranno dalle procedure di gestione e controllo del rischio e comprenderanno 1) la politica di accettazione della clientela, 2) l'identificazione del cliente, 3) il regolare monitoraggio dei conti ad alta rischiosità e 4) la gestione del rischio. Le banche non dovrebbero limitarsi ad accertare l'identità dei clienti, ma dovrebbero anche monitorare i movimenti dei conti al fine di individuare le transazioni che appaiono anomale avuto riguardo al tipo di cliente o di conto. I requisiti KYC dovrebbero costituire un elemento centrale delle procedure di gestione e controllo del rischio ed essere integrati da regolari verifiche di conformità e revisioni interne. La portata dei programmi KYC che vanno oltre questi elementi essenziali dovrebbe essere adeguata al grado di rischio.

1. Politica di accettazione dei clienti

20. Le banche dovrebbero definire chiare politiche e procedure per l'accettazione della clientela, tra cui una descrizione dei tipi di clienti che comportano presumibilmente rischi superiori alla media. A tale riguardo andrebbero considerati fattori come il background, il paese d'origine e la posizione pubblica o di elevato profilo del cliente, la titolarità di conti collegati, l'attività economica svolta e altri indicatori di rischio. Le banche dovrebbero adottare politiche e procedure di accettazione differenziate con requisiti di diligenza progressivamente più stringenti in funzione della rischiosità del cliente. Ad esempio, per l'accensione di un conto da parte di una persona con una normale attività lavorativa e un saldo modesto potrebbe essere prescritta l'osservanza dei requisiti più elementari. È infatti importante che i criteri di accettazione della clientela non siano così restrittivi da precludere l'accesso ai servizi bancari da parte del grande pubblico, e in particolare delle persone economicamente o socialmente sfavorite. Per converso, è essenziale che venga esercitata una scrupolosa diligenza nei confronti di un soggetto con ingenti disponibilità di origine incerta. La decisione di allacciare rapporti di affari con clienti a più alto rischio, come le persone "politicamente esposte" (cfr. sezione 2.2.5), dovrebbe essere presa unicamente a livello di alta direzione.

2. Identificazione del cliente

21. L'identificazione del cliente è un elemento essenziale dei requisiti di diligenza. Ai fini del presente documento si intende per cliente:

---

[5] *Metodologia dei Principi fondamentali per un'efficace vigilanza bancaria*, Criterio essenziale 1.

- ogni persona fisica o giuridica che intrattiene, o nell'interesse della quale è intrattenuto (titolare effettivo), un conto presso la banca;
- il beneficiario di transazioni effettuate da intermediari professionisti;
- ogni persona fisica o giuridica associata a una transazione finanziaria che possa comportare per la banca un rilevante rischio di reputazione o di altro tipo.

22. Le banche dovrebbero istituire una procedura sistematica di identificazione dei nuovi clienti ed evitare di stabilire relazioni finanziarie con essi finché la loro identità non sia stata verificata in modo soddisfacente.

23. Le banche dovrebbero disporre di politiche "documentate e applicate di fatto per l'identificazione dei clienti e dei soggetti che agiscono per loro conto"[6]. I documenti più idonei a verificare l'identità dei clienti sono quelli più difficili da ottenere illegalmente o da contraffare. Particolare attenzione è richiesta nel caso della clientela non residente, e in nessuna circostanza la banca dovrebbe eludere la procedura di identificazione soltanto perché il nuovo cliente non può presentarsi di persona. La banca dovrebbe sempre chiedersi per quale ragione il cliente ha scelto di aprire un conto in una giurisdizione estera.

24. Il procedimento di identificazione del cliente si applica naturalmente all'inizio della relazione. Ma affinché i dati rimangano aggiornati e pertinenti, è necessario che le banche verifichino regolarmente la documentazione esistente[7]. Un momento opportuno per tale verifica è quello in cui viene effettuata una transazione importante, oppure sono modificati in modo significativo gli standard per la documentazione della clientela, oppure interviene un cambiamento sostanziale nel modo in cui è utilizzato un conto. Tuttavia, ogniqualvolta una banca ritenga di non possedere sufficienti informazioni su un dato cliente, essa dovrebbe compiere i passi necessari affinché tutti i dati pertinenti siano ottenuti il più presto possibile.

25. Le istituzioni che offrono servizi di private banking sono particolarmente esposte al rischio di reputazione e dovrebbero pertanto esercitare una più scrupolosa diligenza in questo tipo di operazioni. I conti di private banking, che per loro natura comportano un alto grado di riservatezza, possono essere accesi a nome di un individuo, di un'impresa, di un trust, di un intermediario o di una società di investimento personalizzato. In ognuno di questi casi la banca può esporsi a un rischio di reputazione se non applica con diligenza le procedure di identificazione stabilite. Tutti i nuovi clienti e i nuovi conti dovrebbero essere approvati da almeno una persona di appropriato livello gerarchico, oltre al responsabile delle relazioni di private banking. Qualora per questa sfera di attività siano previste particolari salvaguardie interne a tutela della riservatezza, la banca dovrà comunque assicurarsi che sui clienti e sulle operazioni in questione possano essere esercitati uno scrutinio e un monitoraggio almeno equivalenti, ad esempio mediante verifiche da parte degli addetti al controllo di conformità e dei revisori.

26. Le banche dovrebbero definire "chiare regole che stabiliscono la documentazione da tenersi sull'identificazione del cliente e sulle singole transazioni, nonché il suo periodo di conservazione"[8]. Questa prassi è essenziale affinché le banche possano seguire la relazione con il cliente, conoscere le sue attività correnti e, se necessario, produrre evidenze in caso di controversie, azioni legali o indagini finanziarie che potrebbero sfociare in procedimenti penali. Quale ovvia e naturale prosecuzione della procedura di identificazione, la banca dovrebbe richiedere al cliente i documenti necessari per la sua identificazione e conservarne copia per almeno cinque anni dopo la chiusura del conto. Anche le evidenze di tutte le transazioni finanziarie andrebbero tenute per almeno cinque anni dal giorno in cui hanno avuto luogo.

2.1 Requisiti generali

27. Le banche devono poter ottenere tutte le informazioni ritenute necessarie per stabilire in modo pienamente soddisfacente l'identità di ciascun nuovo cliente, così come la finalità e la prevista

---

[6] *Metodologia dei Principi fondamentali per un'efficace vigilanza bancaria*, Criterio essenziale 2.

[7] L'applicazione di nuovi standard KYC ai conti già esistenti è attualmente all'esame della FATF.

[8] *Metodologia dei Principi fondamentali per un'efficace vigilanza bancaria*, Criterio essenziale 2.

tipologia della relazione finanziaria. La portata e la natura delle informazioni dipenderanno dalle caratteristiche del richiedente (privato, impresa, ecc.) e dalla presunta entità del saldo. Le autorità di vigilanza nazionali sono invitate a fornire criteri guida che assistano le banche nella definizione delle procedure di identificazione. Il Gruppo di lavoro ha intenzione di definire gli elementi essenziali dei requisiti di identificazione della clientela.

28. Allorché un conto è già stato aperto, ma nella relazione bancaria sopravvengono problemi di verifica irrisolvibili, la banca dovrebbe chiudere il conto stesso e restituire i fondi alla fonte da cui le sono pervenuti[9].

29. Sebbene la provenienza delle disponibilità iniziali da un conto intestato al nuovo cliente presso un'altra banca che applica gli stessi standard KYC possa fornire una certa assicurazione, va comunque considerata la possibilità che tale banca abbia preteso l'estinzione del conto a causa di dubbi sulla liceità delle attività svolte dal titolare. Ovviamente, i clienti hanno il diritto di spostare fondi da un istituto all'altro. Tuttavia, se una banca ha motivo di credere che a un richiedente sia stato negato l'accesso ai servizi di un altro istituto, essa dovrebbe applicare nei suoi confronti procedure di diligenza più stringenti.

30. Le banche non dovrebbero mai accettare di aprire un conto o di effettuare operazioni con un soggetto che persista nel mantenere l'anonimato o fornisca un nominativo fittizio. I conti cifrati confidenziali[10] non dovrebbero funzionare come conti anonimi, bensì essere soggetti esattamente alle stesse procedure KYC che si applicano a tutti gli altri conti, quand'anche i controlli siano compiuti da personale selezionato. I conti cifrati possono sì offrire una protezione addizionale per l'identità del titolare, ma questa deve essere nota a un sufficiente numero di funzionari della banca affinché sia esercitata la dovuta diligenza. Tali conti non dovrebbero quindi in nessun caso essere utilizzati per celare l'identità del cliente ai responsabili del controllo interno di conformità o alle autorità di vigilanza.

2.2 Questioni specifiche

31. Restano da affrontare talune questioni più di dettaglio inerenti all'identificazione del cliente. Parte di esse è attualmente all'esame della FATF nel quadro di una revisione generale delle sue 40 Raccomandazioni, e il Gruppo di lavoro riconosce la necessità di un approccio coerente con i principi della FAFT.

2.2.1 Conti intestati a trust, rappresentanti e fiduciari

32. I conti intestati a trust, rappresentanti e fiduciari possono essere utilizzati per eludere le procedure di identificazione. Sebbene in determinate circostanze sia lecito prevedere un margine di sicurezza addizionale per tutelare la riservatezza dei legittimi clienti di private banking, è essenziale che sia ben compresa la vera natura della relazione. Le banche dovrebbero accertare se il cliente assume il nome di un altro soggetto, se agisce da prestanome, oppure se opera per conto di una terza persona in qualità di amministratore fiduciario, rappresentante o in altra veste. In questi casi è indispensabile che la banca ottenga sufficienti evidenze sull'identità dell'intermediario e del soggetto per conto del quale questi agisce, nonché informazioni dettagliate sulla natura del rapporto fiduciario o di rappresentanza. In particolare, il procedimento di identificazione di un trust dovrebbe comprendere gli affidatari (trustees), i disponenti/affidanti (settlors/grantors) e i beneficiari (beneficiaries)[11].

2.2.2 Società veicolo

33. Le banche devono vigilare affinché le imprese societarie non siano utilizzate da persone fisiche come strumento per manovrare conti anonimi. Taluni veicoli di gestione personalizzata di

---

[9] Fatta salva la legislazione nazionale in materia di transazioni sospette.

[10] In un conto cifrato, il nome del titolare è noto alla banca, ma viene sostituito da un codice alfanumerico nella successiva documentazione.

[11] I beneficiari dovrebbero essere per quanto possibile identificati allorché sono individuabili. Si riconosce che non sempre è possibile individuare fin dall'inizio i beneficiari di un trust. Ad esempio, i beneficiari possono essere persone non ancora nate, oppure diventare tali solo al verificarsi di un determinato evento. Inoltre, ai beneficiari rientranti in specifiche categorie (come nel caso di un fondo pensione aziendale) possono essere opportunamente applicati i criteri enunciati per i conti collettivi, di cui ai paragrafi 38-39.

patrimoni, come le società d'affari internazionali, possono rendere difficile la corretta identificazione dei clienti e dei titolari effettivi. Una banca dovrebbe conoscere bene la struttura della società, determinare l'origine dei fondi e individuare i proprietari effettivi o i soggetti che hanno il controllo sui fondi.

34. Particolare cautela deve essere esercitata nell'instaurare relazioni finanziarie con società aventi azionisti prestanome o azioni al portatore. Per le società di questo tipo è essenziale che siano acquisite soddisfacenti evidenze sull'identità dei proprietari effettivi. Nel caso di società con capitale costituito in larga parte da azioni al portatore è richiesta un'accresciuta vigilanza. Una banca può infatti essere del tutto ignara degli eventuali trasferimenti di tali azioni. Spetta alle banche porre in atto efficaci procedure per monitorare l'identità dei proprietari effettivi di portafogli rilevanti. Ciò potrebbe implicare che la banca immobilizzi le azioni, ad esempio trattenendole in custodia.

2.2.3 Clienti introdotti da terzi

35. Le procedure di identificazione possono comportare un dispendio di tempo, ed è naturale che le banche desiderino limitare gli inconvenienti causati alla nuova clientela. Di conseguenza, in alcuni paesi è invalsa l'abitudine di fare assegnamento sulle procedure applicate da altri istituti o da agenti che fungono da referenza per i clienti proposti. Questa prassi comporta tuttavia il rischio che le banche confidino in misura eccessiva nelle procedure di diligenza che esse presumono siano state applicate dai terzi proponenti. Il fatto di contare sull'espletamento degli obblighi di diligenza da parte dell'agente che funge da referenza, per quanto autorevole egli sia, non esime in alcun modo le banche dalla responsabilità di conoscere i propri clienti e le loro attività. In particolare, le banche non dovrebbero fare affidamento su agenti che applicano standard KYC meno rigorosi di quelli su cui sono basate le proprie procedure di identificazione o che non sono disposti a fornire copia della documentazione attestante l'esercizio della dovuta diligenza.

36. Il Comitato di Basilea raccomanda alle banche che si avvalgono di agenti per la presentazione di un cliente di vagliare accuratamente la loro "onorabilità e professionalità" e di assicurarsi che essi esercitino la dovuta diligenza secondo i criteri stabiliti in questo documento. È comunque alla banca che compete la responsabilità ultima di conoscere i propri clienti. Le banche dovrebbero basarsi sui seguenti criteri per stabilire l'idoneità di un agente[12]:

- esso deve conformarsi ai requisiti minimi di diligenza per l'identificazione della clientela stabiliti nel presente documento;
- le procedure di diligenza dell'agente devono essere altrettanto rigorose quanto quelle che avrebbe applicato al cliente la banca stessa;
- la banca deve essere certa dell'affidabilità dei sistemi impiegati dall'agente per verificare l'identità del cliente;
- la banca deve concordare con l'agente di poter verificare in ogni momento se esso ha esercitato la dovuta diligenza;
- tutti i dati identificativi rilevanti e i documenti concernenti l'identità del cliente devono essere immediatamente sottoposti dall'agente alla banca, la quale è tenuta a esaminare accuratamente la documentazione ricevuta. Tali informazioni devono essere accessibili all'autorità di vigilanza e all'organo di investigazione finanziaria, o autorità di polizia equivalente, cui sia stato conferito il necessario potere legale.

Inoltre, la banca che fa ricorso a un agente dovrebbe effettuare periodiche verifiche per assicurarsi che questi continui a conformarsi ai criteri sopra enunciati.

2.2.4 Conti di clienti aperti da intermediari professionisti

37. Allorché una banca sa per certo o ha motivo di ritenere che il conto aperto da un intermediario professionista è gestito in favore di un dato cliente, essa deve pretendere di conoscere l'identità di quest'ultimo.

---

[12] La FATF sta attualmente esaminando i criteri di idoneità da applicare agli agenti che presentano un cliente.

38. Le banche detengono spesso conti “collettivi” gestiti da intermediari professionisti in favore di enti, come fondi comuni di investimento, fondi pensione e fondi cassa. Esse intrattengono anche conti collettivi intestati ad avvocati o agenti di cambio in cui sono versati fondi detenuti in deposito o custodia per vari tipi di clienti. Qualora tali fondi non siano indivisi, bensì ripartiti in “sottoconti” attribuibili a singoli beneficiari, questi ultimi devono essere identificati individualmente.

39. Nel caso in cui i fondi siano indivisi, la banca dovrebbe identificare i beneficiari. Possono esservi circostanze in cui la banca non abbia bisogno di risalire a monte dell’intermediario, come ad esempio quando quest’ultimo è tenuto a osservare le stesse norme e procedure prudenziali e antiriciclaggio e, in particolare, soggiace agli stessi requisiti di diligenza per l’identificazione della clientela. Le autorità di vigilanza nazionali dovrebbero chiaramente definire le circostanze particolari di cui sopra. Le banche dovrebbero accettare tali conti soltanto se sono in grado di appurare che l’intermediario esercita la dovuta diligenza e dispone di sistemi e controlli per allocare gli averi depositati nel conto collettivo ai rispettivi beneficiari. Nel valutare le procedure di diligenza poste in atto dall’intermediario la banca dovrebbe applicare i criteri enunciati nel paragrafo 36 in relazione agli agenti che presentano un cliente, al fine di determinare se l’intermediario stesso offre sufficienti garanzie di affidabilità.

40. Se l’intermediario non è abilitato a fornire alla banca le necessarie informazioni sui beneficiari, come nel caso degli avvocati[13] vincolati dal segreto professionale, oppure non soggiace a requisiti di diligenza equivalenti a quelli stabiliti nel presente documento o alle disposizioni previste dalle norme antiriciclaggio, la banca non dovrebbero consentirgli di aprire un conto.

2.2.5 Persone politicamente esposte

41. Le relazioni d’affari con individui che ricoprono importanti cariche pubbliche e con persone o imprese ad essi chiaramente collegate possono esporre le banche a notevoli rischi di reputazione e/o legali. Con persone “politicamente esposte” (PPE) si intendono gli individui che sono o erano preposti ad alte funzioni pubbliche, come Capi di Stato o di Governo, personalità politiche, quadri superiori della Pubblica amministrazione, della magistratura e delle forze armate, dirigenti di imprese pubbliche e importanti esponenti di partiti politici. Vi è sempre la possibilità, specie nei paesi in cui la corruzione è fenomeno diffuso, che tali persone abusino dei propri poteri per trarre illeciti guadagni da atti di concussione, malversazione, ecc.

42. L’accettazione e gestione di fondi di PPE corrotte reca grave danno alla reputazione della banca e rischia di pregiudicare la fiducia del pubblico negli standard etici di un intero centro finanziario, poiché solitamente i casi del genere sono seguiti con grande attenzione dai media e suscitano forti reazioni politiche, anche se l’origine illecita degli averi è spesso difficilmente comprovabile. Inoltre, le banche possono essere soggette a costose richieste di informazioni e a provvedimenti sequestrativi a opera delle autorità di polizia o giudiziarie (anche nel quadro di procedure di mutua assistenza giuridica internazionale in materia penale), nonché subire azioni per il risarcimento di danni intentate dallo Stato in questione o dalle vittime di un regime. In determinate circostanze, anche la banca stessa e/o i suoi funzionari possono incorrere nell’accusa di riciclaggio di proventi illeciti, ove risulti che sapevano o avrebbero dovuto sapere che i fondi originavano da corruzione o da altri atti delittuosi.

43. Alcuni paesi hanno recentemente modificato, o stanno modificando, la propria normativa al fine di perseguire penalmente la corruzione attiva di funzionari pubblici esteri in linea con la relativa convenzione internazionale[14]. In tal modo, gli atti di corruzione all’estero vengono a configurare una presunzione di reato in materia di riciclaggio di fondi illeciti, attivando l’applicazione di tutte le prescrizioni antiriciclaggio (come la segnalazione di transazioni sospette, il divieto di informare il cliente, il congelamento interno di fondi, ecc.). Ma anche in difetto di una tale base esplicita di diritto penale, è chiaramente indesiderabile, eticamente scorretto e incompatibile con i requisiti di onorabilità e di professionalità che una banca accetti o mantenga una relazione finanziaria qualora essa sappia o debba presumere che i fondi traggono origine da corruzione, concussione o peculato. Per una banca

---

[13] La FATF sta rivedendo le procedure KYC da applicarsi ai conti aperti da avvocati su incarico dei clienti.

[14] Si veda la Convenzione OCSE su *Combating Bribery of Foreign Public Officials in International Business Transactions*, adottata dalla Negotiating Conference il 21 novembre 1997.

che stia considerando una relazione d'affari con un individuo che essa supponga essere una PPE è una necessità imprescindibile identificare pienamente tale individuo, nonché le persone e le imprese ad esso chiaramente collegate.

44. Le banche dovrebbero ottenere sufficienti informazioni dall'interessato e verificare le informazioni disponibili pubblicamente per stabilire se il nuovo cliente sia o meno una PPE. In caso affermativo le banche dovrebbero accertare l'origine dei fondi prima di acconsentire all'accensione di un conto. La decisione in merito dovrebbe essere presa a livello di alta direzione.

2.2.6 Clienti non conosciuti di persona

45. Alle banche è sempre più spesso richiesto di aprire conti a favore di clienti che non si presentano di persona. Il fenomeno, che in passato riguardava tipicamente la clientela non residente, negli ultimi tempi ha assunto assai maggiore importanza con la diffusione dei servizi bancari postali, telefonici ed elettronici. Le banche dovrebbero sottoporre tale clientela "remota" agli stessi requisiti di identificazione e di monitoraggio continuativo applicati ai clienti con i quali ha un contatto diretto. Una questione sorta in tale contesto riguarda la possibilità di una verifica indipendente a opera di una parte terza di chiara fama. L'intera problematica inerente all'identificazione della clientela remota viene attualmente discussa in seno alla FATF, oltre a essere oggetto di esame nel quadro dell'emendamento della Direttiva CEE del 1991.

46. Un tipico esempio di cliente remoto è la persona che intenda effettuare operazioni bancarie elettroniche tramite Internet o tecnologie analoghe. I servizi bancari elettronici comprendono ormai una vasta gamma di prodotti offerti in rete. La natura impersonale e transnazionale di tali servizi, congiunta alla loro rapidità di esecuzione, crea inevitabilmente problemi per l'identificazione e la verifica del cliente. Come principio fondamentale, le autorità di vigilanza si attendono che le banche valutino attivamente i vari rischi posti dalle tecnologie emergenti e applichino procedure di identificazione che tengono adeguatamente conto di tali rischi[15].

47. Sebbene la medesima documentazione possa essere prodotta dalla clientela conosciuta di persona e dalla clientela remota, nel caso di quest'ultima il riscontro dell'identità risulta ovviamente più difficile. Nelle operazioni bancarie telefoniche ed elettroniche il problema della verifica è reso ancora più acuto.

48. Allorché vengono accettati clienti remoti le banche devono:

- applicare procedure di identificazione altrettanto rigorose quanto quelle impiegate per la clientela disponibile a un contatto diretto;
- porre in atto adeguate misure specifiche per attenuare il maggiore rischio.

Sono esempi di misure dirette ad attenuare il rischio:

- certificazione dei documenti presentati;
- richiesta di documenti addizionali rispetto a quelli prescritti alla clientela conosciuta di persona;
- presa di contatto con il cliente su iniziativa autonoma della banca;
- referenze di terzi, ad esempio da parte di un agente soggetto ai requisiti stabiliti al paragrafo 36;
- richiesta che il primo versamento sia effettuato tramite un conto intestato al cliente presso un'altra banca che applica gli stessi requisiti di diligenza.

2.2.7 Servizi bancari di corrispondenza

49. Per servizi bancari di corrispondenza si intende la prestazione di servizi da parte di una banca ("banca mandataria") per conto di un'altra banca ("banca mandante"). I conti di corrispondenza, ampiamente utilizzati su scala mondiale, consentono alle banche di offrire prodotti e servizi che esse

[15] L'Electronic Banking Group del Comitato di Basilea ha pubblicato nel maggio 2001 un rapporto sui principi di gestione del rischio nei servizi bancari elettronici.

non sono in grado di fornire direttamente. Fra i conti di corrispondenza richiedono particolare attenzione quelli che prevedono l'offerta di servizi in giurisdizioni in cui la banca mandante non ha alcuna presenza fisica. In ogni caso, le banche che omettono di applicare a tali conti i dovuti criteri di diligenza si espongono ai vari tipi di rischio sopra descritti e possono venirsi a trovare nella situazione di detenere e/o trasferire fondi collegati a corruzione, frode o altri atti illeciti.

50. Le banche dovrebbero acquisire sufficienti informazioni sulle proprie mandanti al fine di conoscere pienamente la natura delle loro operazioni. Fra gli aspetti da considerare figurano: informazioni concernenti la direzione della banca mandante, le principali attività da essa svolte e la loro localizzazione, nonché le misure messe in atto per prevenire e individuare il riciclaggio di fondi illeciti; le finalità del conto; l'identità di eventuali terzi che utilizzano i servizi bancari di corrispondenza; la qualità della regolamentazione e della vigilanza bancaria nel paese di insediamento. Le banche dovrebbero stabilire rapporti di corrispondenza con istituzioni estere soltanto se queste sono efficacemente vigilate dalle rispettive autorità. Per parte loro, le banche mandanti dovrebbero applicare rigorose politiche e procedure per l'identificazione e l'accettazione della clientela.

51. In particolare, le banche dovrebbero rifiutare di iniziare o continuare un rapporto di corrispondenza con un'istituzione che abbia sede legale in una giurisdizione nella quale non è materialmente presente e che non sia affiliata a un gruppo finanziario regolamentato ("società di comodo"). Le banche dovrebbero essere particolarmente vigili allorché intrattengono rapporti di corrispondenza con istituti situati in giurisdizioni che non applicano rigorosi requisiti KYC o che sono state designate come "non cooperative" nella lotta contro il riciclaggio di capitali illeciti. Le banche dovrebbero assicurarsi che le proprie corrispondenti applichino i requisiti di diligenza stabiliti nel presente documento in ordine alle operazioni effettuate tramite i conti di corrispondenza.

52. Le banche dovrebbero considerare con particolare attenzione il rischio che i conti di corrispondenza siano utilizzati direttamente da terzi per effettuare operazioni per proprio conto (ad esempio, tramite conti di transito). Per tali meccanismi valgono sostanzialmente le considerazioni applicabili alle operazioni di clienti introdotti su presentazione, e quindi i criteri stabiliti al paragrafo 36.

3. Monitoraggio continuativo dei conti e delle operazioni

53. Il monitoraggio continuativo è una componente essenziale di un rigoroso sistema di procedure KYC. Le banche possono controllare e ridurre efficacemente il rischio soltanto se conoscono la normale e ragionevole movimentazione dei conti dei propri clienti, così da poter individuare le operazioni che si discostano dal profilo consueto. Senza una tale conoscenza esse possono facilmente mancare al dovere di segnalare le operazioni sospette alle autorità appropriate nei casi in cui sono tenute a farlo. La portata del monitoraggio deve essere commisurata al rischio. Per tutti i conti le banche dovrebbero avere in funzione sistemi idonei a individuare attività insolite o sospette. A questo fine possono essere stabiliti limiti di importo per le operazioni in ciascuna classe o categoria di conti, il cui superamento dovrebbe essere considerato con particolare attenzione. Anche certi tipi di operazioni dovrebbero mettere in allerta la banca per la possibilità che il cliente stia svolgendo attività insolite o sospette. Tali sono, ad esempio, le operazioni che non appaiono plausibili dal punto di vista economico o commerciale, oppure che comportano depositi in contante di grande ammontare non giustificati dalla normale e prevedibile attività del cliente. Un'eccessiva movimentazione, non commisurata all'entità del saldo, potrebbe indicare che i fondi sono stati "riciclati" attraverso il conto. Una casistica esemplificativa delle attività sospette può essere di notevole aiuto alle banche e dovrebbe far parte delle procedure e/o direttive adottate da una giurisdizione per la lotta al riciclaggio di proventi illeciti.

54. Il monitoraggio dovrebbe essere rafforzato per i conti a più alto rischio. Ogni banca dovrebbe stabilire indicatori chiave per questi conti, avendo riguardo a vari aspetti, come il paese d'origine del cliente, la provenienza dei fondi, il tipo di operazioni effettuate e altri fattori di rischio. Per i conti in questione:

- le banche dovrebbero assicurarsi di disporre di adeguati sistemi informativi per la direzione, affinché ai dirigenti e ai responsabili del controllo di conformità siano forniti con tempestività i dati necessari per identificare, analizzare e sorvegliare efficacemente i movimenti del conto. Fra le segnalazioni potenzialmente necessarie figurano eventuali lacune nella documentazione prescritta per l'apertura del conto, operazioni a valere sul conto di un cliente che appaiono anomale e presentazione complessiva di tutti i rapporti del cliente con la banca;

- i quadri superiori preposti ai servizi di private banking dovrebbero conoscere bene il profilo soggettivo dei clienti ad alto rischio e seguire con attenzione le fonti di informazioni esterne che li concernono. Le operazioni importanti disposte da questi clienti dovrebbero essere approvate da un alto dirigente;
- le banche dovrebbero definire una chiara politica, fissare direttive, procedure e controlli interni ed esercitare una vigilanza particolare riguardo alle relazioni d'affari con le PPE e i soggetti di elevato profilo, nonché con le persone e le imprese a essi chiaramente collegate o associate[16]. Data la possibilità che non tutte le PPE siano individuate come tali fin dall'inizio, o che clienti esistenti acquisiscano soltanto in seguito questo status, dovrebbero essere compiute verifiche regolari almeno della clientela più importante.

4. Gestione del rischio

55. Un efficace programma KYC comprende procedure per un'adeguata supervisione direzionale, sistemi e controlli appropriati, separatezza delle funzioni, formazione professionale e altri aspetti collegati. Il consiglio di amministrazione della banca dovrebbe assumere il fermo impegno di attuare un rigoroso programma KYC, stabilendo le procedure appropriate e accertandosi della loro efficacia. All'interno della banca dovrebbero essere assegnate esplicite responsabilità per assicurare che le direttive e le procedure fissate vengano seguite correttamente e siano quantomeno conformi alle prescrizioni di vigilanza locali. I canali per la segnalazione delle operazioni sospette dovrebbero essere chiaramente specificati in forma scritta e resi noti a tutto il personale. Dovrebbero inoltre essere previste procedure interne per determinare se gli obblighi contemplati dalla normativa sulla segnalazione delle attività sospette impongano alla banca di notificare una data operazione alle competenti autorità di polizia, giudiziarie e/o di vigilanza.

56. Alle funzioni di audit interno e di controllo di conformità competono importanti responsabilità nel valutare e assicurare l'osservanza delle direttive e procedure KYC di una banca. Come regola generale, la funzione di controllo di conformità dovrebbe effettuare una valutazione indipendente di tali direttive e procedure, tenuto conto della normativa legale e di vigilanza. Fra i suoi compiti dovrebbe rientrare il monitoraggio continuativo dell'operato del personale mediante verifiche a campione e l'esame delle deroghe, allo scopo di allertare l'alta direzione e il consiglio di amministrazione qualora ritenga che i quadri responsabili non applichino le procedure KYC in modo rigoroso.

57. L'audit interno ha un ruolo importante nel valutare in modo autonomo i sistemi di gestione e controllo del rischio, riferendo al collegio dei sindaci o ad analogo organo di supervisione, mediante relazioni periodiche sull'osservanza delle politiche e procedure KYC, comprese quelle concernenti la formazione del personale. La direzione dovrebbe assicurarsi che la funzione di audit sia adeguatamente dotata di personale competente nella materia in questione. Inoltre, il personale preposto a tale funzione dovrebbe interessarsi attivamente al modo in cui viene dato seguito alle sue osservazioni e critiche.

58. Tutte le banche devono attuare un regolare programma di formazione del personale affinché questo sia adeguatamente addestrato nelle procedure KYC. Tempi e contenuti della formazione per le diverse categorie di personale saranno necessariamente adattati alle esigenze particolari della singola banca. L'impostazione dei corsi differirà a seconda che si tratti di nuovi assunti, operatori di sportello, addetti al controllo di conformità e personale che tratta con i nuovi clienti. Il personale di nuova assunzione deve essere sensibilizzato sull'importanza delle procedure KYC e sui principi fondamentali cui si ispira la banca. I dipendenti di front-office a diretto contatto con il pubblico dovrebbero essere istruiti a verificare l'identità dei nuovi clienti, a espletare su base regolare gli obblighi di diligenza nella gestione dei conti della clientela esistente e a discernere forme di attività sospette. Dovrebbero inoltre essere organizzati regolari corsi di aggiornamento, affinché il personale abbia sempre ben presenti le

[16] Non è realistico attendersi che la banca sia informata o indaghi su ogni lontana relazione familiare, politica o finanziaria di un cliente estero. Le esigenze investigative dipenderanno dalla dimensione o dal movimento dei beni, dalla tipologia delle operazioni, dal background economico, dalla reputazione del paese, dalla plausibilità delle spiegazioni fornite dal cliente, ecc. Va tuttavia notato che le PPE (o meglio, i loro familiari e amici) non si presenteranno necessariamente in tale veste, ma piuttosto come normali professionisti (seppure agiati), dissimulando il fatto che devono la loro posizione elevata in un'impresa legittima unicamente alla relazione privilegiata che intrattengono con il titolare della carica pubblica.

proprie responsabilità e sia informato sui nuovi sviluppi. È essenziale che tutto l'organico interessato comprenda appieno la necessità delle politiche KYC e le applichi in modo rigoroso. Una cultura aziendale che promuova questa comprensione è determinante ai fini di un'efficace attuazione di tali politiche.

59. In molti paesi anche i revisori esterni svolgono un ruolo importante nel monitorare le procedure e i controlli interni delle banche e nell'attestare che essi sono conformi alle prescrizioni di vigilanza.

IV. Ruolo delle autorità di vigilanza

60. Basandosi sugli standard internazionali esistenti, le autorità di vigilanza nazionali dovrebbero emanare direttive intese a disciplinare i programmi KYC delle banche. Gli elementi essenziali enunciati in questo documento dovrebbero fornire alle autorità un chiaro orientamento su come definire o perfezionare la normativa prudenziale nazionale in materia.

61. Oltre a stabilire i requisiti basilari cui devono conformarsi le banche, le autorità di vigilanza sono chiamate ad accertare che queste applichino corrette procedure KYC e operino costantemente nel rispetto degli standard etici e professionali. Le autorità di vigilanza dovrebbero assicurarsi che le banche dispongano di adeguati controlli interni e ottemperino alle prescrizioni prudenziali e regolamentari. Il processo di vigilanza dovrebbe contemplare non soltanto lo scrutinio delle politiche e procedure, ma anche un esame dei dossier clienti e una verifica campionaria dei conti. Le autorità di vigilanza dovrebbero sempre avere la facoltà di accedere a tutta la documentazione relativa ai conti detenuti nella propria giurisdizione, comprese le eventuali analisi effettuate dalla banca per individuare operazioni anomale o sospette.

62. Le autorità di vigilanza hanno il dovere di assicurarsi che le banche di propria pertinenza applichino elevati standard KYC non soltanto al fine di proteggere la sicurezza e la solidità delle singole aziende, ma anche per preservare l'integrità dell'intero sistema bancario nazionale[17]. Le autorità dovrebbero far chiaramente intendere che adotteranno le misure appropriate – le quali potranno essere severe e rese note al pubblico, se opportuno – contro le banche e i loro dipendenti che in modo comprovabile violano le direttive interne o le prescrizioni regolamentari. Inoltre, esse dovrebbero assicurarsi che le banche individuino e trattino con particolare cautela le operazioni inerenti a giurisdizioni in cui vigono standard ritenuti inadeguati. La FATF e alcune autorità nazionali hanno predisposto una specifica dei paesi e delle giurisdizioni i cui ordinamenti legali e amministrativi sono considerati non conformi agli standard internazionali per la lotta al riciclaggio di fondi illeciti. Tali indicazioni dovrebbero essere integrate nelle politiche e procedure KYC di una banca.

V. Applicazione dei requisiti KYC in un contesto transnazionale

63. Le autorità di vigilanza di tutto il mondo dovrebbero porre il massimo impegno nel definire e attuare nella propria giurisdizione standard KYC che siano pienamente in linea con i requisiti internazionali, al fine di evitare potenziali "arbitraggi" regolamentari e salvaguardare l'integrità del sistema bancario a livello interno e internazionale. L'attuazione e lo scrutinio di tali standard sono un banco di prova della disponibilità degli organi di vigilanza a cooperare fra di loro in modo concreto e della capacità delle banche di controllare i rischi a livello di gruppo. Si tratta di un compito impegnativo, cui sono chiamate tanto le istituzioni creditizie quanto le autorità di vigilanza.

64. Le autorità di vigilanza si attendono che i gruppi bancari applichino uno standard minimo riconosciuto per le politiche e le procedure KYC sia alle operazioni sull'interno che a quelle transfrontaliere. La supervisione dell'attività bancaria internazionale può essere esercitata in modo efficace soltanto su base consolidata, e i rischi di reputazione e di altro genere non sono confinati al

[17] In molti paesi le autorità di vigilanza sono parimenti tenute a segnalare eventuali operazioni sospette, anomale o illegali che esse rilevino, ad esempio, nel corso di ispezioni in loco.

territorio nazionale. Affinché i programmi KYC operino efficacemente a livello globale, le case madri devono comunicare le proprie politiche e procedure alle filiali e filiazioni estere, ivi comprese entità non bancarie come le società fiduciarie, e predisporre controlli di routine per verificare l'ottemperanza agli standard del paese d'origine e del paese ospitante. Tali controlli di conformità saranno anche sottoposti allo scrutinio dei revisori esterni e delle autorità di vigilanza, ed è quindi importante che la connessa documentazione sia opportunamente conservata e disponibile per i relativi accertamenti. Ai fini della verifica di conformità, gli organi di vigilanza e i revisori esterni dovrebbero in linea generale esaminare i sistemi e i controlli in funzione, nonché i conti della clientela e il monitoraggio delle operazioni nel quadro di accertamenti campionari.

65. Indipendentemente dalle dimensioni della dipendenza estera, dovrebbe essere designato un quadro superiore direttamente responsabile di assicurare che tutto il personale interessato conosca e applichi procedure KYC conformi ai requisiti sia del paese ospitante che del paese d'origine. Sebbene spetti a tale funzionario la responsabilità primaria di questo compito, egli dovrebbe essere coadiuvato dai revisori interni e dagli addetti alla conformità in forza presso la dipendenza stessa ovvero la sede centrale.

66. Qualora i requisiti minimi KYC del paese d'origine e del paese ospitante non siano uniformi, le filiali e filiazioni situate in quest'ultima giurisdizione dovrebbero applicare gli standard più elevati. In generale, non dovrebbero esservi impedimenti a che una banca adotti standard superiori ai requisiti minimi prescritti in loco. Se tuttavia le leggi e i regolamenti del paese ospitante (specie le norme di segretezza) interdicono l'applicazione degli standard KYC del paese d'origine allorché questi sono più restrittivi, le autorità di vigilanza del paese ospitante dovrebbero adoperarsi affinché la normativa nazionale venga modificata. Nel frattempo, le filiali e filiazioni estere dovrebbero conformarsi ai requisiti locali, assicurandosi però che la sede centrale o casa madre e le autorità di vigilanza del paese di quest'ultima siano pienamente informate sulla natura delle difformità.

67. Gli elementi criminali sono facilmente attirati verso le giurisdizioni in cui vigono impedimenti del genere. Pertanto, le banche dovrebbero essere consapevoli del forte rischio di reputazione cui si espongono svolgendo attività in tali giurisdizioni. Le case madri dovrebbero disporre di procedure per analizzare la vulnerabilità delle singole unità operative e predisporre, ove appropriato, salvaguardie addizionali. In casi estremi, le autorità di vigilanza dovrebbero considerare l'opportunità di esercitare controlli aggiuntivi sulle banche attive nelle giurisdizioni in questione e, se del caso, incoraggiare il loro ritiro dalle stesse.

68. Durante le ispezioni in loco le autorità di vigilanza e i revisori del paese d'origine non dovrebbero incontrare nessun ostacolo nell'accertare la conformità della dipendenza con le politiche e procedure KYC. Ciò implicherà l'esame dei registri dei clienti e verifiche a campione di singoli conti. Gli organi di controllo dovrebbero avere accesso alle informazioni sui singoli conti in misura sufficiente a consentire un'adeguata valutazione degli standard KYC applicati e delle procedure di gestione del rischio, senza che vi ostino le norme locali sul segreto bancario. Qualora le autorità del paese d'origine prescrivano la segnalazione consolidata delle concentrazioni dei depositi e dei fidi o la notifica dei fondi in amministrazione, non dovrebbero esservi impedimenti a comunicare tali dati. Inoltre, per poter sorvegliare le concentrazioni dei depositi o i rischi di provvista in relazione ai prelievi, le autorità del paese d'origine potrebbero applicare test di rilevanza o stabilire determinate soglie limite, cosicché le banche siano tenute a segnalare i depositi di singoli clienti superiori a una certa quota percentuale del totale di bilancio. Sono tuttavia necessarie salvaguardie per assicurare che le informazioni su singoli conti vengano utilizzate esclusivamente per legittimi fini prudenziali e possano essere protette in modo soddisfacente da parte di chi li riceve. A questo riguardo, sarebbe utile un protocollo di mutua collaborazione[18] per facilitare lo scambio di informazioni fra le autorità di vigilanza delle due giurisdizioni.

69. In certi casi può sussistere un serio conflitto fra le politiche KYC della casa madre imposte dall'autorità di vigilanza nazionale e le attività permesse a una sua dipendenza all'estero. Può accadere, ad esempio, che la legislazione locale non permetta ispezioni da parte dei responsabili del controllo di conformità, dei revisori interni o degli organi di vigilanza dell'istituzione madre, o consenta ai clienti di utilizzare nomi fittizi o di celarsi dietro rappresentanti o intermediari cui è fatto divieto di

[18] Si veda il documento del Comitato di Basilea *Essential elements of a statement of cooperation between banking supervisors* (maggio 2001).

rivelare l'identità dei propri clienti. In tali casi l'autorità del paese d'origine dovrebbe comunicare con l'autorità del paese ospitante al fine di appurare se esistono effettivi impedimenti legali e se questi si applicano extra-territorialmente. Qualora gli ostacoli si rivelino insormontabili e non siano possibili alternative soddisfacenti, l'autorità del paese d'origine dovrebbe far chiaramente intendere alla sua omologa che la banca potrebbe decidere, autonomamente o su richiesta dell'autorità stessa, di chiudere la dipendenza in questione. In definitiva, qualsiasi accordo a sostegno di tali ispezioni in loco dovrebbe prevedere meccanismi atti a consentire una valutazione che sia soddisfacente per l'autorità del paese d'origine. A tale riguardo, possono essere utili dichiarazioni di cooperazione o protocolli d'intesa che stabiliscano i meccanismi di questi accordi. L'accesso alle informazioni da parte del paese d'origine dovrebbe essere il più possibile libero da restrizioni e permettere, come minimo, l'accertamento delle politiche e procedure generali della banca in relazione al dovere di diligenza nell'identificazione dei clienti e nel trattamento dei casi sospetti.

Allegato 1

Estratto dal documento *Metodologia dei Principi fondamentali per un'efficace vigilanza bancaria*

Principio 15: Le autorità di vigilanza bancaria devono poter accertare che le banche applicano politiche, prassi e procedure (compresi criteri rigorosi in merito alla conoscenza del cliente) tali da promuovere un elevato standard etico e professionale nel settore finanziario e da impedire che la banca si presti, con o senza intenzionalità, a essere utilizzata da elementi criminali.

Criteri essenziali

1. L'autorità di vigilanza accerta che le banche dispongano di adeguate politiche, prassi e procedure per promuovere un elevato standard etico e professionale e per impedire che la banca si presti, con o senza intenzionalità, a essere utilizzata da elementi criminali. Ne fanno parte la prevenzione e l'individuazione di attività criminose o frodi e la segnalazione di tali attività sospette alle autorità competenti.
2. L'autorità di vigilanza accerta che le banche dispongano, nel quadro dei programmi antiriciclaggio, di politiche documentate e applicate di fatto per l'identificazione dei clienti e dei soggetti che agiscono per loro conto. Esistono chiare regole che stabiliscono la documentazione da tenersi sull'identificazione del cliente e sulle singole transazioni, nonché il suo periodo di conservazione.
3. L'autorità di vigilanza accerta che le banche dispongano di procedure formali per l'individuazione delle transazioni potenzialmente sospette. Tali procedure possono prevedere autorizzazioni addizionali per i depositi e prelievi in contante (o simili) di grande ammontare e procedimenti speciali per le transazioni inusuali.
4. L'autorità di vigilanza accerta che le banche designino un alto funzionario avente la responsabilità esplicita di assicurare che le politiche e le procedure della banca siano come minimo conformi alle prescrizioni legali e regolamentari locali in materia di lotta al riciclaggio di capitali.
5. L'autorità di vigilanza accerta che le banche dispongano di procedure chiare, rese note a tutto il personale, per la segnalazione interna delle transazioni sospette al funzionario responsabile della conformità con la normativa antiriciclaggio.
6. L'autorità di vigilanza accerta che le banche abbiano istituito linee di comunicazione sia verso la direzione che verso la funzione di sicurezza interna per la segnalazione dei casi problematici.
7. Oltre a riferire alle competenti autorità giudiziarie, le banche segnalano alle autorità di vigilanza le attività sospette e gli atti di frode rilevanti ai fini della sicurezza, della solidità e della reputazione della banca.
8. Le leggi, i regolamenti e/o le politiche delle banche assicurano che i dipendenti i quali segnalano in buona fede transazioni sospette al dirigente preposto, alla funzione di sicurezza interna o direttamente all'autorità competente non possano essere ritenuti responsabili di violazione di obblighi.
9. L'autorità di vigilanza verifica periodicamente che i controlli antiriciclaggio delle banche e i loro sistemi per prevenire, individuare e segnalare le frodi siano sufficienti. L'autorità di vigilanza dispone di adeguati poteri coercitivi (promovimento di azione civile e/o penale) per agire nei confronti di una banca che non si conformi alle prescrizioni antiriciclaggio.
10. L'autorità di vigilanza è in grado, direttamente o indirettamente, di scambiare con altre istanze di controllo del settore finanziario nazionali o estere informazioni inerenti a presunte o effettive attività criminose.

11. L’autorità di vigilanza accerta che le banche abbiano adottato una dichiarazione di principi in materia di etica e comportamento professionali comunicata in termini chiari a tutto il personale.

Criteri integrativi

1. Le leggi e/o i regolamenti incorporano i principi internazionali per una corretta prassi, come le 40 Raccomandazioni della Financial Action Task Force (FATF/GAFI) emanate nel 1990 (rivedute nel 1996).
2. L’autorità di vigilanza accerta che il personale delle banche sia adeguatamente addestrato in materia di individuazione e prevenzione del riciclaggio di denaro.
3. L’autorità di vigilanza è tenuta per legge a segnalare alle competenti autorità penali ogni transazione sospetta.
4. L’autorità di vigilanza è in grado, direttamente o indirettamente, di scambiare con le competenti autorità giudiziarie informazioni inerenti a presunte o effettive attività criminose.
5. Ove la funzione non sia espletata da altro organo, l’autorità di vigilanza dispone di risorse interne con competenze specialistiche in materia di frode finanziaria e di prescrizioni antiriciclaggio.

Allegato 2

Estratto dalle Raccomandazioni FATF/GAFI

C. Ruolo del sistema finanziario nella lotta al riciclaggio dei fondi di provenienza illecita

Regole per l'identificazione dei clienti e la tenuta della documentazione

10. Le istituzioni finanziarie non dovrebbero intrattenere conti anonimi o intestati a nomi manifestamente fittizi: esse dovrebbero essere tenute (in forza di leggi, regolamenti, accordi fra le autorità di vigilanza e le istituzioni finanziarie o accordi di autoregolamentazione fra le istituzioni finanziarie) a identificare i clienti, sia occasionali che usuali, sulla base di un documento di riconoscimento ufficiale o di altro documento affidabile, e a registrarne le generalità, allorché stabiliscono relazioni d'affari o effettuano operazioni (in particolare, apertura di conti o depositi, esecuzione di transazioni fiduciarie, locazione di cassette di sicurezza, operazioni in contante di grande ammontare).

    Al fine di adempiere i requisiti di identificazione concernenti le persone giuridiche, le istituzioni finanziarie dovrebbero, ove necessario, adottare misure per:

    (i) verificare l'esistenza e la struttura giuridica del cliente, ottenendo da un pubblico registro o dal cliente stesso, ovvero da entrambi, prova della costituzione in società, corredata di informazioni concernenti la ragione sociale, la forma giuridica, la sede, gli amministratori e le disposizioni che regolano la capacità di obbligare legalmente l'ente;

    (ii) verificare se ogni persona che affermi di agire in nome del cliente sia a ciò autorizzata e identificare tale persona.

11. Le istituzioni finanziarie dovrebbero adottare misure ragionevoli per ottenere informazioni sulla vera identità delle persone in favore delle quali è aperto un conto o effettuata un'operazione se vi è ragione di dubitare che il cliente stia agendo per proprio conto, come ad esempio nel caso delle società di comodo (ossia istituzioni, società, fondazioni, trust, ecc. che non svolgono alcuna attività commerciale o industriale, né hanno altre forme di operatività nel paese in cui è situata la loro sede legale).

12. Le istituzioni finanziarie dovrebbero conservare per almeno cinque anni tutta la necessaria documentazione sulle operazioni compiute, sia nazionali che internazionali, affinché possano essere soddisfatte prontamente eventuali richieste di informazioni da parte delle autorità competenti. La documentazione deve essere sufficiente a permettere la ricostruzione delle singole operazioni (compresi gli importi e i tipi di moneta, se del caso) così da fornire, ove necessario, elementi di prova per il perseguimento di comportamenti delittuosi.

    Le istituzioni finanziarie dovrebbero conservare la documentazione relativa all'identificazione del cliente (ad esempio, copie o annotazioni dei documenti di riconoscimento ufficiali come passaporti, carte d'identità, patenti di guida o simili), i registri dei conti e la corrispondenza commerciale per almeno cinque anni dalla data di chiusura del conto.

    Questa documentazione dovrebbe essere a disposizione delle autorità nazionali competenti nel caso di procedimenti o istruttorie penali.

13. I paesi dovrebbero dedicare particolare attenzione ai pericoli di riciclaggio di capitali insiti nelle tecnologie nuove o in evoluzione idonee a favorire l'anonimato e dovrebbero, ove necessario, adottare provvedimenti per impedire il loro utilizzo come canali di riciclaggio.

Accresciuta diligenza delle istituzioni finanziarie

14. Le istituzioni finanziarie dovrebbero dedicare particolare attenzione a tutte le operazioni complesse e di ammontare insolitamente elevato, nonché a tutti i tipi di operazioni che non hanno una palese finalità economica o uno scopo legittimo visibile. Per quanto possibile, dovrebbero essere analizzati gli aspetti sottostanti e il fine di tali operazioni; i risultati dell'analisi dovrebbero essere documentati per iscritto e tenuti a disposizione delle autorità di vigilanza, dei revisori e degli organi giudiziari e di polizia.

15. Allorché le istituzioni finanziarie sospettano che i fondi provengano da un'attività criminale, esse dovrebbero essere tenute a segnalare prontamente tali sospetti alle autorità competenti.

16. Le istituzioni finanziarie e i loro amministratori, funzionari e dipendenti dovrebbero essere protetti in forza di legge da ogni responsabilità penale o civile per violazione dei vincoli di riservatezza – siano essi imposti per contratto o da disposizioni legali, regolamentari o amministrative – allorché segnalano in buona fede i propri sospetti alle autorità competenti, quand'anche non sappiano esattamente di quale fattispecie criminosa si tratti e prescindendo dal fatto che risulti esservi effettivamente stata un'attività illecita.

17. Le istituzioni finanziarie e i loro amministratori, funzionari e dipendenti non dovrebbero avvertire o, se del caso, essere autorizzati ad avvertire i clienti del fatto che informazioni che li riguardano sono state trasmesse alle autorità competenti.

18. Le istituzioni finanziarie che segnalano operazioni sospette dovrebbero conformarsi alle istruzioni delle autorità competenti.

19. Le istituzioni finanziarie dovrebbero porre in essere programmi contro il riciclaggio di denaro che prevedano come minimo:

    (i) la definizione di politiche, procedure e controlli interni, ivi compresa la designazione di responsabili per il controllo di conformità a livello di direzione, e adeguate procedure di selezione per assicurare standard elevati in sede di assunzione del personale;

    (ii) un programma continuativo di formazione del personale;

    (iii) una funzione di audit per verificare il sistema.