ABI Associazione Bancaria Italiana

Position Paper in risposta alla procedura di consultazione della Banca d'Italia "Sistema dei controlli interni, sistema informativo e continuità operativa"

Novembre 2012

POSITION PAPER

Sommario

Premessa

Il presente Position Paper dell'Associazione Bancaria italiana è strutturato come segue:

- commenti generali
- risposte ai quesiti posti dalla Banca d'Italia (box)
- singoli paragrafi su argomenti specifici nei quali con commenti, richieste di modifiche e richieste di chiarimenti.

In considerazione della molteplicità dei temi trattati dalla consultazione sono stati interessati i seguenti Gruppi di Lavoro interbancari ABI: Funzione Compliance, Compliance Finanza, Rischio Operativo, Commissione Permanente Rischi Bancari (questa ultima in particolare per le questioni inerenti le Funzioni di Risk Management e di Internal Auditing), Vigilanza, Imposte dirette, Imposte indirette e fiscalità finanziaria, Società.

In ambito ABI Lab hanno contribuito il Consiglio Direttivo del Consorzio e i gruppi di lavoro interbancari: Osservatorio Business Continuity, Osservatorio Sicurezza e Frodi Informatiche.

Si ringrazia la Banca d'Italia per la disponibilità mostrata durante alcuni incontri preliminari di chiarimento e si rimane a disposizione per ulteriori approfondimenti.

Principali punti di attenzione

A livello generale emergono due principali considerazioni:

A) il documento, sebbene in alcuni ambiti specifici soddisfi le richieste di chiarimento in termini di criteri organizzativi di massima da adottare, ***definisce talora requisiti minimi organizzativi stringenti*** *(es.* assegnazione di responsabilità, collocazione delle funzioni e delle unità) e ***spesso non riscontrabili nelle scelte organizzative da tempo adottate dalle banche*** e in qualche caso già approvate dalle Autorità di Vigilanza. Prima di confermare alcune delle previsioni vincolanti di cui sopra, tra i diversi aspetti da considerare si auspica che, in osservanza al **principio di economicità**, si verifichi che i **costi di adeguamento organizzativo** siano commisurati ai **vantaggi reali** conseguibili in termini di rafforzamento di alcune funzioni specifiche e più in generale del presidio dei rischi aziendali nel quadro del sistema dei controlli interni.

B) il documento appare una integrazione delle diverse normative esistenti mentre riterremmo necessaria una maggiore razionalizzazione e semplificazione della materia. Si pensi, ad esempio, al tema della sovrapposizione tra funzione compliance e internal audit alla luce del Regolamento Congiunto Banca d'Italia - Consob sui servizi di investimento nonché al difficile coordinamento tra le funzioni dell'Organismo di Vigilanza e quelle delle altre funzioni di controllo nelle materie disciplinate dal d.lgs 231/01.

Per ciascuna delle due categorie di considerazioni prima illustrate, si sintetizzano sotto alcuni dei principali punti emersi, poi approfonditi nei rispettivi paragrafi.

A)

- Una novità di rilievo è l'attribuzione alla funzione di compliance della verifica di conformità dell'attività aziendale alle normative di natura fiscale per evitare di incorrere in violazioni o elusioni di tale normativa ovvero in situazioni di abuso del diritto. La necessità di strutturare nell'ambito del sistema dei controlli interni presidi idonei alla gestione e al controllo del rischio fiscale è condivisa dalle banche, in particolare quelle di maggiori dimensioni, che già adottano tali presidi. Sul tema, come peraltro ricordato nel documento di consultazione, è all'esame al Parlamento un disegno di legge delega che contempla per i soggetti di grandi dimensioni la previsione di sistemi aziendali strutturati di gestione e di controllo del rischio fiscale, con una chiara attribuzione di responsabilità nel quadro del complessivo sistema dei controlli interni. Ciò posto, per evitare il rischio che, con la delega in corso di attuazione, gli intermediari finanziari si trovino di fronte a disposizioni di vigilanza non coerenti, in tutto o in parte, con la normativa di attuazione della richiamata legge delega, si propone di attendere il completamento, previsto in tempi brevi, del relativo processo attuativo. Le banche, in particolare quelle di maggiori dimensioni, sono comunque disponibili a confrontarsi con la Banca d'Italia sui presidi già adottati per la gestione e il controllo del rischio fiscale per valutarne la coerenza con le esigenze dell'Organo di Vigilanza;
- in tema di conformità dei complessi processi di Vigilanza Prudenziale, anche alla luce di alcuni provvedimenti sanzionatori dell'Autorità di Vigilanza, il documento in consultazione dovrebbe meglio chiarire la suddivisione dei ruoli tra funzione di compliance e altre funzioni specialistiche (fatta eccezione per quanto esplicitamente

attribuito alla funzione di convalida per le banche adoperanti sistemi avanzati per la determinazione dei requisiti minimi patrimoniali). In ottica di efficacia ed efficienza, visto il *know how* necessario, nonché in linea con il principio di proporzionalità, si richiede di lasciare agli intermediari autonomia in materia di connesse scelte organizzative e quindi si richiede di enucleare la Vigilanza Prudenziale dal novero delle aree normative necessariamente e completamente allocate sotto la responsabilità, per quanto attiene al rischio di non conformità, della funzione compliance. Le succitate scelte organizzative potrebbero spaziare[1] i) dalla inclusione nel perimetro della funzione di conformità di alcuni fra i processi di Vigilanza Prudenziale ii) ad una responsabilità limitata alla fase di disegno/validazione del *framework* di gestione del connesso rischio di non conformità (ed eventualmente alla sua periodica verifica). In questo ultimo caso alle funzione specialistiche (es. risk management ma anche funzioni non di controllo) andrebbe la responsabilità di attuare tale *framework* (ossia la concreta opera di identificazione, valutazione/misurazione, monitoraggio ed attenuazione secondo il disegno definito dalla funzione di conformità e approvato dagli organi aziendali);

- sempre in tema di funzione di conformità, il documento non chiarisce se la responsabilità della funzione compliance si estenda anche a quelle normative per le quali la legislazione vigente impone la presenza di specifiche figure aziendali che riportino alle strutture di vertice dell'azienda (ad esempio, la normativa in materia di sicurezza sul lavoro e la continuità operativa). In tali casi si ritiene che alla funzione di compliance sia affidata esclusivamente la verifica che le suddette figure aziendali siano state correttamente identificate;
- nel quadro complessivo assolutamente condivisibile del **rafforzamento** del ruolo della **funzione di controllo rischi** (criteri di nomina e revoca, pareri preventivi, possibilità di riferire direttamente agli organi di vertice), si ritiene necessaria una rivisitazione di uno degli elementi connessi all'indipendenza di tale funzione, che pure si ritiene fondamentale. Ci si riverisce al paragrafo in cui viene inserito il concetto di "**dirette dipendenze"**. Dovendosi interpretare tale concetto come differenziale rispetto a "riferiscono direttamente" (prevista in altre parti del documento) lo si è inteso non in senso funzionale, bensì gerarchico. In questa accezione l'obbligatorietà di una collocazione gerarchica presso gli organi di vertice appare una previsione caratterizzata da una eccessiva rigidità organizzativa (proponiamo che dovrebbe rimanere per tutte le banche una opzione e non deve diventare una imposizione). Infatti, in talune realtà una collocazione gerarchica presso gli organi di vertice potrebbe rendere la funzione di controllo dei rischi avulsa dal business, mentre in altre ne potrebbe in effetti garantire una maggiore efficacia;
- un approccio analogo viene proposto anche per declinare meglio il termine "presiedere" attribuito alla funzione compliance con riferimento alle normative diverse da quelle rilevanti;
- si richiede flessibilità su un aspetto di particolare rilevanza, ossia le soluzioni organizzative che prevedono la figura del *Chief Risk Officer* **(CRO)** inteso, presso molte realtà, come **figura di supervisione/coordinamento di autonome e separate funzioni (di controllo rischi, funzione di conformità ed eventuali altre funzioni)** Ovviamente, l'istituzione della figura CRO non è e non dovrà mai essere considerato un obbligo: ciò

[1] A tal proposito è già stato reso disponibile alla Banca d'Italia un documento scaturente dai lavori del tavolo ABICS Compliance Knowledge Center sul tema "Eventuali possibili ruoli della Funzione Compliance nei processi di Vigilanza Prudenziale".

non di meno, si richiede all'Organo di Vigilanza una valutazione/interpretazione dei possibili ruoli delle diverse funzioni di controllo in presenza di questa nuova figura organizzativa e delle inter-relazioni che ne scaturiscono, le quali si tiene possano contribuire a delineare l'auspicato percorso di una visione sempre più integrata dei rischi;

- alla luce del divieto per i responsabili delle funzioni di controllo di avere responsabilità diretta di funzioni operative sottoposte a controllo, si chiede di confermare che la struttura che **gestisce i reclami** non debba essere considerata una struttura operativa dell'intermediario e possa pertanto dipendere gerarchicamente dal responsabile della funzione di compliance;
- con riferimento **all'Organismo di Vigilanza** si ritiene fondamentale che le disposizioni, in linea con il disposto del d.lgs 231/01, e nel rispetto del principio di economicità, riconoscano **maggiore flessibilità organizzativa** alle banche nella individuazione dell'organo titolare delle funzioni dell'Odv;
- con riferimento al **governo e organizzazione dell'*Information and Communication Technology*** (ICT) e alle misure di sicurezza da adottare, si sottolinea in particolare l'obbligo da parte dell'organo con funzione di supervisione strategica di deliberare "in ordine al modello di riferimento per l'architettura dei sistemi informativi"; a tale riguardo emerge fra gli Associati la necessità di chiarire come gli organi aziendali debbano interagire con un eventuale *outsourcer* cui sia affidata la gestione del sistema informativo;
- riguardo al neo istituito "**Direttore dei sistemi informativi** o equivalente", si ritiene troppo vincolante rispetto alle autonome scelte organizzative la previsione di un riporto gerarchico diretto di tale figura verso l'organo con funzione di gestione;
- in merito alla definizione e collocazione del **processo di analisi del rischio informatico** e della funzione a ciò preposta, emerge la necessità di maggiore chiarezza, in particolare riguardo il processo di analisi e gestione del rischio informatico: la proposta normativa sembra avallare l'impostazione che inquadra nell'"utente responsabile" la figura di riferimento cui delegare tale attività, senza dare la giusta evidenza alla **funzione di sicurezza informatica**, oggi presente nell'assoluta maggioranza delle banche;
- per le banche con approccio di vigilanza *home – host* è importante prevedere la possibilità di mantenere un approccio flessibile sull'assetto organizzativo delle funzioni di controllo, in coerenza con quello delle banche estere capogruppo, atto a garantire a livello di gruppi internazionali l'omogeneità delle soluzioni organizzative in tema di controlli interni. Si chiede di valutare se, avuto riguardo all'esigenza di assicurare un rapporto ottimale costi/benefici nell'articolazione e nella conduzione dei controlli, la declinazione del principio di proporzionalità possa prevedere anche la possibilità di non istituire la funzione di revisione interna laddove l'organizzazione dei controlli di 1° e 2° livello e le caratteristiche dell'attività lo consentano per quelle entità che, facendo parte di un Gruppo Bancario, sono comunque soggette / assoggettabili a controlli di revisione interna da parte della Capogruppo sulla base di un sistema di controllo di terzo livello integrato e omogeneo per l'intero Gruppo. Ciò comporterebbe infatti il beneficio di un'organizzazione della revisione interna integrata nel Gruppo bancario, la quale utilizzerebbe risorse proprie direttamente presso l'entità sulla base del piano di audit risk based (eliminando peraltro gli oneri connessi alla nomina di un referente per l'internal audit interno all'entità del Gruppo). In tal caso verrebbe meno l'applicazione

di ogni previsione relativa all'esternalizzazione della funzione di revisione interna per le entità dello stesso Gruppo Bancario.

B)

- la descrizione del **ruolo degli organi aziendali** viene ampliamente riportata nel Tit. V, Cap. 7, Sezione II; non appare evidente la motivazione per cui esista un ulteriore riferimento nel Tit. V, Cap 8, Sezione II specificatamente al governo e organizzazione dell'ICT. Tale scelta, forse dettata dalla volontà di creare un documento modulare, non appare efficace, crea un disequilibrio tra le altre parti in cui una analoga sezione non è prevista e sembrerebbe oggettivamente contraria all'obiettivo di razionalizzare la materia in una sorta di testo unico del Sistema dei Controlli Interni. Quanto meno servirebbe una sorta di tavola sinottica che posizionata nel Tit. V, Cap. 7, Sezione II, indichi in quali altri punti vengono richiamati i ruoli degli organi aziendali;
- in tema **di nomina e revoca dei Responsabili delle funzioni di controllo** il documento dispone che essi siano nominati e revocati (motivandone le ragioni) **dall'organo con funzione di gestione**, d'accordo con l'organo con funzione di supervisione strategica, sentito l'organo con funzione di controllo. La disposizione non è coerente con quanto previsto nell'ambito delle "Disposizioni sul Governo Societario" (Banca d'Italia – 04.03.2008) secondo cui "la nomina del responsabile delle Funzioni di revisione interna e di conformità rientra tra le attribuzioni del CDA non delegabili";
- con riguardo **all'organo con funzione di gestione**, si segnala come a questo spetti, secondo il documento, di definire il processo diretto alla **distribuzione di nuovi prodotti di investimento** attraverso cui, in particolare, dovrebbero essere definite le fasce di clientela a cui si intendono distribuire nuovi prodotti o servizi in relazione alla complessità degli stessi e ad eventuali vincoli normativi. Appare opportuno che tale previsione vada resa **coerente con quanto previsto dalla vigente regolamentazione CONSOB** in tema di obblighi di valutazione di adeguatezza a carico degli intermediari;
- appare problematica la completa assenza di informativa sul coordinamento della **funzione antiriciclaggio** con le altre funzioni di controllo;
- **in tema di esternalizzazione delle funzioni di controllo** si richiede di impostare in modo differenziato le previsioni contenute nella relativa sezione a seconda di esternalizzazioni **infragruppo** o esternalizzazione verso **terzi**. Si auspica che emerga la differenza tra **accentramento** ed **esternalizzazione**. Si tratta infatti di circostanze assai eterogenee che devono essere valorizzate anche in ottemperanza al principio di economicità. Va poi considerato afferente alla sfera infragruppo anche la categoria di esternalizzazioni verso strutture del medesimo network;
- con riferimento ai controlli interni di gruppo, si ritiene inefficiente e scarsamente efficace il **riporto gerarchico di referenti periferici** (oltre che in sé non prevedibile per risorse appartenenti a società giuridiche diverse). Ciò in particolare, secondo il criterio di proporzionalità, in gruppi bancari che detengono un limitato numero di entità, le quali assumono rischi rilevanti nel solo territorio nazionale;
- sempre con riferimento ai controlli interni di gruppo, si osserva che l'istituzione di una **unità di revisione interna deputata ad effettuare in via esclusiva controlli**

su base individuale per le controllate sarebbe fonte di diseconomie e se ne chiede quindi **l'eliminazione**. Tra l'altro il criterio prevalente di specializzazione delle risorse di auditing è per ambito/processo e tale impostazione garantisce efficacia ed efficienza certamente maggiore di quella per singola entità o per capogruppo vs entità controllate;

- le manifestazioni del rischio informatico appartengono al più ampio spettro di quelle del rischio operativo. La identificazione, valutazione/misurazione, mitigazione e monitoraggio di tale rischio richiedono professionalità specifiche che non risiedono generalmente nella funzione risk management (in cui spesso è presente una funzione dedicata al rischio operativo, l'Orm). **In ottica di efficienza**, sarebbe auspicabile che venisse esplicitamente richiamata l'opportunità di una stretta **collaborazione tra l'owner del rischio informatico** (non inquadrato come funzione di controllo di secondo livello e quindi non richiamato nel paragrafo 5 - Cap. 7 Sezione II) **e la funzione di risk management/Orm**; ad esempio, le attività di raccolta dati di perdita e le valutazioni di scenari di rischio sono spesso già svolte dalla funzione Orm anche con riferimento ai sistemi informativi;
- in materia di **continuità operativa**, la proposta normativa integra ed abroga la precedente normativa in materia di *Business Continuity*; tra i principali elementi di novità si evidenzia in particolare l'inserimento del **processo di erogazione del contante** tra quelli a rilevanza sistemica, rivolto sia alle singole banche sia alle infrastrutture di sistema: si richiede di considerare sistemica l'infrastruttura e non i singoli punti di erogazione o gruppi di essi;
- inoltre, la fase di revisione della normativa sulla continuità operativa può rappresentare l'occasione per proporre di modificare parti del testo già presenti nei testi originari, ma che, alla luce dell'esperienza maturata in questi otto anni di normativa, potrebbero essere meglio precisati: a questo riguardo il competente gruppo di lavoro ha identificato opportunità di modifica degli scenari da considerare nella predisposizione dei piani di continuità e delle modalità di esecuzione delle verifiche del piano.

* * *

- **Con rifermento ai tempi di attuazione delle nuove Disposizioni** si rileva che essi non sono indicati nel documento in consultazione. Pertanto si chiede che, una volta pubblicato il documento definitivo, sia concesso un congruo periodo di tempo (6 mesi) per una **attenta pianificazione in capo a ciascun intermediario degli interventi da effettuare per allinearsi alla nuova normativa**. In relazione ai **tempi di implementazione** delle attività e dei presidi individuati in fase di pianificazione si reputa che essi dipendano, oltre che dalla situazione di gap di ciascun intermediario, dalla risoluzione di alcune delle criticità sopra evidenziate. Non essendo quindi possibile esprimere una stima a livello di settore, si auspica che la **ragionevolezza dei tempi di implementazione** indicati in fase di realizzazione sia oggetto di **riflessioni tra l'intermediario e a Banca d'Italia**. Certamente per alcuni aspetti particolarmente impattanti i tempi di implementazione potrebbero superare i 12 mesi;
- infine, si richiede a Banca d'Italia di **armonizzare le previsioni in consultazione con i tempi di rilascio di altre normative a livello internazionale** per non creare uno svantaggio competitivo agli intermediari Italiani (es. previsioni sul leverage

ratio o sulla risk data aggregation). Potrebbe essere presa in considerazione l'ipotesi di date di pubblicazione o entrata in vigore ancorate alla emanazione delle norme correlate.

Risposte ai Box

1. Determinazione della tolleranza al rischio/appetito per il rischio (Capitolo 7, Sezione II, par. 2)

Box 1

La tolleranza al rischio (*risk tolerance*) e l'appetito per il rischio (*risk appetite*) sono entrambi utilizzati per descrivere sia il livello assoluto di rischio che una banca è a priori disposta ad assumere, sia i limiti effettivi che essa pone nell'ambito di tale livello massimo.

Al fine di valutare l'opportunità di individuare parametri utilizzabili per determinare il livello di rischio assumibile, si sollecita l'indicazione delle variabili quantitative e qualitative correntemente utilizzate o in via di sviluppo per addivenire a tale determinazione.

Quale prima considerazione, anche dalla lettura del documento che accompagnava quello in consultazione, parrebbe opportuno soffermarsi meglio sui concetti non sempre intercambiabili di risk tolerance (inteso in senso lato come limite) e risk appetite (inteso più come rischio target)[2].

In particolare si chiede di modificare il testo del Titolo V, Capitolo 7, Sezione 2, Par 2:

- da "definisce ed identifica il livello di rischio accettato (c.d. "tolleranza al rischio" o "appetito al rischio")";
- in **"definisce il livello di propensione al rischio appropriato ("appetito al rischio") in funzione della natura degli obiettivi strategici, identificandone contestualmente i limiti di tolleranza ("tolleranza al rischio")"**.

* * *

Al fine di supportare il sistema bancario Italiano ad un utilizzo sempre più sostanziale del concetto di Risk Appetite, elemento base del processo decisionale, l'ABI ha approfondito

[2] Si riportano alcuni riferimenti definitori che sottolineano la differenza tra i due termini.
Dal documento di analisi impatto regolamentare sul documento in consultazione SCI di Bankit
"L'espressione risk tolerance/appetite viene utilizzata in modo diverso dalle differenti istituzioni e autorità. Nell'ambito della disciplina dei controlli interni i due termini sono utilizzati per descrivere sia i rischi assoluti che un'istituzione è disposta ad assumere a priori (risk appetite) sia quelli effettivi (risk tolerance). Dotarsi di un "risk appetite framework" vuol dire, pertanto, definire gli obiettivi di rischio che la banca intende e può raggiungere e tradurli in vincoli e incentivi per la struttura aziendale.".
Risk Management ISTAT
Natura e livello degli obiettivi devono essere allineati con l'orientamento all'accettazione e gestione dei rischi (risk appetite) definiti dai vertici dell'organizzazione; in questo modo si può definire la tolleranza per il rischio ammissibile all'interno dell'organizzazione (risk tolerance).
COSO - ERM Framework
La risk tolerance rappresenta l'applicazione del risk appetite a specifici obiettivi. Risk appetite è un concetto ampio che rappresenta il livello di rischio che l'entità è disposta ad assumere in relazione agli obiettivi strategici preposti. La risk tolerance è tattica e operativa e deve essere espressa in termini misurabili in relazione all'obiettivo da raggiungere, ad un obiettivo di alto livello di risk appetite, corrispondono diversi livelli di risk tolerance per ogni tipologia di obiettivo definito

tale tema, attraverso un apposito gruppo di lavoro interbancario[3] istituito nel periodo settembre – novembre 2010[4].

Relativamente a uno dei quattro capitoli del documento ossia "B. Metodologia / processo di definizione del Risk Appetite" si riporta di seguito una sintesi delle evidenze emerse[5], in quanto rappresenta sostanzialmente - alla data del 2010 - una risposta al box 1 della consultazione.

In prima approssimazione si era definito il Risk Appetite come l'ammontare massimo di capitale che una banca è disposta a mettere a disposizione per la copertura dei rischi a fronte di un determinato rendimento atteso.
La definizione del Risk Appetite può assumere varie forme e diversi livelli di complessità.

Di seguito viene illustrata quello che si concordò potesse essere una possibile linea evolutiva:

- Definizione Base
  - Tier 1 ratio o, prudenzialmente, livelli più stringenti
- Definizione con KPI quantitativi
  - Capitale economico e probabilità di default
  - Mix per tipologia di rischio
  - Volatilità dei profitti
  - Capitale a rischio
  - Excess Capital
  - Earning at Risk
  - ….
- Integrazione con KPI qualitativi
  - Target Rating per la Banca
  - Rating della controparte
  - Black list di paesi in cui investire
  - Asset classes (e.g. no derivati di credito)
  - …
- Definizione Rischio -Rendimento
  - Rendimento atteso a fronte del capitale allocato
  - …
- Definizione Pluriennale
  - Definizione di Risk Appetite che incorpori l'evoluzione attesa del profilo di rischio-rendimento e di business della banca

[3] Quanto emerso nei tavoli tecnici è stato raccolto in un report denominato "Il Processo di definizione e gestione del Risk Appetite nelle Banche Italiane" – Gruppo di Lavoro "Risk Appetite" – Marzo 2011, già reso disponibile alla Banca d'Italia.
[4] Il gruppo di lavoro, coordinato dall'Ufficio Analisi e Gestione dei rischi dell'ABI, si è avvalso della collaborazione della società di consulenza Bain & Company Italy.
[5] In particolare sono sintetizzate le evidenze raccolte nei Capitolo "B.1 Definizione con KPI quantitativi e qualitativi", "B.2 Tipologie di definizione del Risk Appetite" del report "Il Processo di definizione e gestione del Risk Appetite nelle Banche Italiane – Gruppo di Lavoro "Risk Appetite" – Marzo 2011".

Stante questo quadro concettuale di riferimento, nel 2010 le banche del gruppo di lavoro indicavano come concretamente utilizzati una serie di indicatori quantitativi e qualitativi per la misura del Risk Appetite, ossia:

- Indicatori **Quantitativi**:
  - Capitale economico e probabilità di default (della banca): il capitale disponibile o specifico sia sufficiente ad assorbire una perdita di una determinata consistenza
  - Volatilità dei profitti: probabilità che le perdite superino una determinata percentuale dei profitti in un anno
  - Capitale a rischio: probabilità che le perdite superino una determinata percentuale current net assets (a fair value) dell'anno successivo
  - Perdita di valore del portafoglio bancario e impatto sul margine a fronte di shock deterministici sui tassi di interesse
  - Elementi dello Stato patrimoniale: capitale che eccede il capitale regolamentare
  - Definire il livello di liquidità desiderato

- Indicatori **Qualitativi**:
  - Rating: livello di rating obiettivo[6], che con opportune tecniche può essere calcolato anche per una banca priva di rating esterno
  - Preferenze di rischio non misurabili: caratteristiche di certi rischi che le banche non vogliono accettare, e.g. attività con un elevato livello di rischio, escludere alcuni Stati , alcuni settori o tipologie di controparti, tipologie di prodotti di investimento (es. CDO) etc.

* * *

Nel corso della procedura di consultazione sono emerse ulteriori riflessioni, rispetto a quanto era stato evidenziato nel documento del Gruppo di Lavoro, che sono di seguito riportate.

1. La declinazione concreta e operativamente riscontrabile del concetto appetito al rischio richiede l'individuazione di uno schema quantitativo che ne permetta la sua identificazione e misurazione su basi oggettive.
   Idealmente, questo obiettivo si potrebbe conseguire disponendo di un **unico indicatore** sintetico di esposizione al rischio e di relative soglie, la cui definizione identifica il grado di appetito assoluto, **definito ex-ante** dalla banca in sede di pianificazione strategica.
   D'altra parte, i **rischi** a cui è esposto un intermediario, anche solo limitandosi a quelli di primo pilastro (mercato, credito/controparte e operativo), hanno natura differente e richiedono *framework* di misurazione **disomogenei** tra di loro (anche dal punto di vista normativo), che non è agevole sintetizzare in unico indicatore di rischio.

2. Una tecnica, sovente adottata nell'ambito del risk management in questi casi è di creare un **indice di rischio sintetico** come combinazione di indicatori di rischio di natura diversa, opportunamente normalizzati. I **coefficienti ponderali** di ciascun rischio sono

[6]Tra gli indicatori qualitativi viene riportato il rating che però può essere inquadrato anche come indicatore quantitativo nel caso di espressione mediante valori quali la probabilità di default (PD).

di entità crescente in base ad un predefinito ed **opportuno sistema di soglie**, che tende quindi a conferire maggiore peso ai tipi di rischio che ne evidenziano una maggiore assunzione.
Questo approccio, che presuppone l'identificazione di indicatori per i singoli segmenti di rischio, non necessariamente tra loro omogenei, offre il vantaggio di disporre di un unico indicatore sintetico di esposizione al rischio complessivamente considerato che, in funzione della disponibilità dei dati relativi agli indicatori di rischio specifico, può essere calcolato anche su base continuativa.
Lo svantaggio principale di questa soluzione è costituito dalla potenziale difficoltà di interpretazione di tale indicatore, che, rappresentando una sintesi di più rischi, potrebbe risultare non immediatamente riconducibile alle esposizioni generate dalle singole classi di rischio.

Alternativamente, la soglia di tolleranza al rischio potrebbe essere determinata da un **panel di indicatori, non aggregati tra di loro**, e da relativi limiti specifici. In questo caso, vengono stabiliti, per ogni tipologia di rischio , degli **indicatori di tolleranza e dei valori soglia, pertanto il grado di appetito al rischio è individuato dai singoli livelli-soglia stabiliti ed il livello massimo di rischio assumibile potrebbe essere individuato in base al numero di tali indicatori che superano le soglie individuate**, eventualmente anche in relazione al corrispondente grado di superamento. Gli indicatori dei singoli rischi dovrebbero essere individuati tra i parametri che già gli intermediari vigilati calcolano a fini regolamentari e normativi, in modo da agevolare la quantificazione del concetto di appetito al rischio e la sua comparabilità tra diversi intermediari.

3. Si riporta un esempio dei parametri utilizzati per singolo rischio:
   - Rischio di credito e controparte: requisito patrimoniale
   - Rischio Operativo: requisito patrimoniale
   - Rischio di mercato: requisito patrimoniale combinato con il Var
   - Rischio di concentrazione "single name": metodologia prevista dall'Allegato B del Titolo III Capitolo 1 della Circolare 263 di Banca d'Italia.
   - Rischio di concentrazione geo-settoriale: metodologia elaborata dal "Laboratorio Rischio di concentrazione" organizzato dall'ABI.
   - Rischio Tasso di interesse: modello interno che si basa su un'analisi di sensitivity.
   - Rischio liquidità operativa: modello basati su una maturity ladder.
   - Rischio liquidità strutturale: rapporto tra volumi di raccolta ed impieghi, sia complessivi che specifici della clientela core.
   - Rischio residuo: approccio qualitativo che si focalizza si presidi adottati
   - Rischio derivante da cartolarizzazioni: approccio qualitativo
   - Rischio strategico: approccio qualitativo che si concentra su processi, definizione degli obiettivi, presidi e reporting
   - Rischio reputazionale: approccio qualitativo basato su una griglia che ne individua gli aspetti rilevanti e le aree di vulnerabilità associate

4. Da un punto di vista di **processo**, la definizione del Risk Appetite in alcune realtà parte con il budget, come nel seguito descritto.
   Si consideri un Risk Appetite espresso in termini di Core Tier 1 e Total Capital Ratio.

Prudenzialmente si fissano a livelli più stringenti di quelli della vigilanza, poi vengono declinati dei limiti dettagliati per rischio e per quantità di patrimonio di vigilanza allocato.
Nel mese x di un determinato anno, si simula il preconsuntivo e si lavora al budget per l'anno successivo e allo sviluppo del piano per il quadriennio seguente. In sede di preconsuntivo/budget/piano si individuano anche le evoluzioni degli assorbimenti patrimoniali e l'evoluzione e del patrimonio di vigilanza.
Vengono simulati gli assorbimenti a fronte del rischio di credito, mercato, operativo, tasso, concentrazione *single name*. Si determina la loro incidenza sul patrimonio di vigilanza. In funzione dei dati che emergono da queste analisi si propone la revisione del documento quadro sui rischi per confermare/aggiornare i limiti specificati (almeno una volta all'anno).
Il budget prevede anche uno sviluppo dell'equilibrio finanziario del Gruppo che andrà valutato in funzione della soglia di tolleranza definita sul rischio di liquidità espressa sia come orizzonte temporale di un mese, sia come limiti in termini di riserve di titoli e liquidità operativa da detenere.
Il processo viene monitorato trimestralmente in sede di comitato di direzione/rischi.

Proposte e quesiti

Proposte
In coerenza con il **principio di proporzionalità**, si propone per le banche di minore dimensione e complessità operativa (es. terza classe ICAAP o quarta macro-categoria SREP) **l'individuazione di parametri comunemente utilizzati nelle prassi aziendali quali, ad esempio**: Core Tier 1 Ratio, Total Capital Ratio ovvero analogo Ratio che includa anche i rischi di Secondo pilastro.

Quesito 1
Con riferimento alla tolleranza al rischio (**risk tolerance**) e all'appetito per il rischio (**risk appetite**), è ammissibile che la banca possa determinare un certo livello di **rischio di conformità** che è disposta ad assumere?

Quesito 2
I parametri utilizzati per la gestione del **rischio operativo** di una banca che utilizza metodologie TSA prevedono che a fronte di una quantificazione del requisito patrimoniale vi sia una valutazione soggettiva/oggettiva delle esposizioni (risultanze Risk Self Assessment e Loss Data Collection). In tale contesto si rende necessario avere indicazioni su come sviluppare una **risk tolerance** in grado di coniugare gli aspetti quantitativi con quelli qualitativi. In particolare per il rischio informatico, gestito all'interno del rischio operativo, può essere fissata in via qualitativa nel rispetto di un livello di tolleranza generale?

2. Identificazione delle operazioni di maggior rilievo oggetto del parere preventivo della funzione di controllo dei rischi (Capitolo 7, Sezione II, parr 2 e 3; Sezione III, par. 3.3)

Box 2
Si sollecitano commenti volti a individuare criteri qualitativi e quantitativi sulla base dei quali identificare le operazioni di maggior rilievo.

Si condivide il principio secondo il quale i **criteri** per la identificazione delle operazioni di maggior rilievo debbano essere **autonomamente individuati dalla banca** (cfr. Organo con funzione di supervisione strategica…. definisce …..punto c) i criteri per individuare le operazioni di maggiore rilievo da sottoporre al vaglio preventivo della funzione di controllo dei rischi (cfr. Sezione III, par. 3.3.), indicando l'estensione, i limiti e le modalità di esercizio dei poteri di detta funzione).

Al riguardo si precisa che l'intervento, della Funzione di controllo dei rischi finalizzato al rilascio del parere preventivo, integra il processo decisionale inerente le operazioni di maggiore rilievo arricchendone la visione dialettica.
Il primo elemento di giudizio da parte della Funzioni di Risk Management è costituito da una esame di coerenza complessiva della "singola operazione di maggiore rilievo" rispetto alle varie Policy di Rischio adottate della Banca.

In quest'ottica, **il parere** preventivo da parte del Risk Management, **non** deve assumere carattere di **ridondanza rispetto** a quello formulato dai **soggetti che propongono l'assunzione del rischio,** bensì deve concorrere ad arricchirne la prospettiva di giudizio, in quanto formulato nella più ampia dimensione sistemica del complesso dei rischi; una prospettiva di valutazione diversa e complementare finalizzata a cogliere le eventuali relazioni ed i connessi effetti che la singola operazione potrebbe determinare in termini di altri vettori di rischiosità anche non misurabili, ancorché valutabili.
Si pensi a titolo meramente esemplificativo alle connessione e agli effetti di amplificazione che una determinata operazione di impiego inerente il Banking Book potrebbe generare, in relazione alla propria struttura e dimensione, non solo in termini di rischi di credito, ma anche in termini di rischio di concentrazione, di liquidità, di tasso di interesse, operativo e reputazionale.
L'aspetto da valorizzare sarebbe, dunque, quello di evitare un processo decisionale, in cui fosse assente una "visione olistica" capace di cogliere i mutevoli aspetti della multidimensionalità dei rischi evitando, al contempo, un approccio meramente "a blocchi" che si è rilevato in molti casi limitante e foriero di pregiudizi ai fini della stabilità del singolo intermediario.

Inoltre, le valutazioni della Funzione di Controllo dei Rischi potrebbero essere ulteriormente arricchite da analisi di scenario o di prove di carico idonee a testare gli eventuali effetti che "una operazione di maggiore rilievo" potrebbe comportare in condizioni avverse anche con riguardo alla tenuta del sistema dei limiti e alla più ampia capacità di resilienza della Banca.

In tal senso l'apporto della Funzione di Risk Management assume carattere di peculiare specificità definendo una area di esclusività in termini di ruolo e di rango organizzativo.

Ciò premesso **una misura** idonea per identificare le "operazioni di maggiore rilievo" **potrebbe essere rappresentata dall'apporto marginale che, la potenziale operazione, potrebbe produrre in termini di assorbimento del livello di "RISK TOLERANCE**", prescelto dall'Organo di Supervisione Strategica; ciascun intermediario nell'ambito delle proprie policy declinerà, seppur in termini frazionali, l'entità di tale incidenza, definendo, al contempo, il processo organizzativo in cui i principi sopra delineati trovano compiuta formalizzazione.
La metrica proposta essendo, quindi espressa in termini di "RISK TOLERANCE", si pone come punto di sutura concettuale, in quanto analoga a quella utilizzata dall'Organo di Supervisione Strategica, che è il destinatario del "parere preventivo" .

Un ulteriore potrebbe essere rappresentato dalla percentuale di assorbimento del Capitale Interno (singolo rischio) e del Capitale Interno Complessivo che l'operazione di particolare rilievo potrebbe determinare.

Solo al fine di creare, nell'ambito dell'autonomia di ogni intermediario, una sorta di minimo comune denominatore si potrebbero considerare operazioni di maggior rilievo quelle:

- messe in essere con Parti Correlate e Soggetti Collegati come definite dal Titolo V, Capitolo 5 della Circolare 263 della Banca D'Italia e che al contempo superino una certa soglia di importo;
- che assumono carattere di straordinarietà, quali acquisizioni di un ramo d'azienda, o di aziende, piuttosto che acquisizioni/cessioni di partecipazioni di controllo, etc.

3. Declinazione del principio di proporzionalità (Capitolo 7, Sezione III, par. 1)

Box 3

La bozza di disciplina, in linea con il principio di proporzionalità, consente alle banche di accorpare ovvero esternalizzare le funzioni di controllo.
Si sollecitano commenti per declinare nel concreto tale principio, sulla base di criteri riferiti alla dimensione e alla complessità operativa delle banche nonché avuto riguardo all'esigenza di assicurare un rapporto ottimale costi/benefici nell'articolazione e nella conduzione dei controlli.

Il tema della proporzionalità, quanto mai opportuno in ottica di efficacia ed efficienza, è di estrema rilevanza in quanto taglia trasversalmente il progetto di implementazione e verifica del sistema dei controlli interni.

Come contributo alle domande poste, può essere utile ricordare come l'ESMA, nel suo documento ***"Orientamenti su alcuni aspetti dei requisiti della funzione di controllo della conformità di cui alla MiFID",*** del settembre scorso, suggerisca alcuni criteri attraverso i quali le imprese di investimento dovrebbero decidere quali misure siano maggiormente adeguate per garantire l'efficacia della funzione di controllo della conformità alla luce delle circostanze particolari dell'impresa.

Un altro criterio di declinazione del principio di proporzionalità potrebbe essere rappresentato dalle **macro-categorie individuate a fini SREP dalla Banca d'Italia**.

Nelle varie possibili soluzioni esplorate, sembrerebbero esservi spesso i due criteri della complessità dimensionale e di quella operativa. Rispetto alla prima si possono annoverare, ad esempio, il fatturato, il numero dei dipendenti, il numero dei canali di vendita, il numero di dipendenze.
La **complessità operativa**, a sua volta, è legata al numero di business line su cui si è attivi e alla distribuzione di alcuni indicatori tra le business line attive; ulteriore indice di complessità può essere rappresentato dalla notevole dotazione di risorse umane e tecnologiche per l'ingresso in un determinato business, tale da costituire una barriera all'ingresso per altri concorrenti, operatività transfrontaliera.

Un ulteriore approccio che potrebbe essere preso in considerazione è quello di rifarsi alla stessa metrica utilizzata per le domestic SIFIs[7]. (intese come intermediari sistematicamente rilevanti a livello EU e/o area Euro). Più in dettaglio oltre a categorizzare gli intermediari italiani appartenenti a tale categoria come una delle classi di proporzionalità, gli stessi criteri adottati per la loro identificazione potrebbero essere "scalati" in basso di ulteriori due o tre livelli per ottenere la identificazione di altri due o tre gruppi. Di tale approccio si apprezza in particolare il fatto di essere equilibrato sulle diverse dimensioni prese in considerazione. Ad esempio, si attribuisce correttamente importanza alla complessità,

[7] Basel Committee on Banking Supervision – "A framework for dealing with domestic systemically important banks" - October 2012

solitamente presa meno in considerazione rispetto alla dimensione.

4. Interazioni tra rischio informatico e rischi operativi (Capitolo 8, Sezione II, par. 1)

Box 4

Sulla base di eventuali esperienze maturate o valutazioni svolte circa l'analisi del rischio informatico e la definizione di livelli di tolleranza per il rischio aziendale, si sollecitano commenti circa le modalità di integrazione delle valutazioni inerenti il rischio informatico nel contesto generale di governo della variabile informatica e di gestione dei rischi operativi

In un contesto bancario dove la componente tecnologica rappresenta un rilevante fattore di produzione, è importante, come evidenziato dall'impianto normativo, definire la corretta sinergia tra la valutazione del rischio informatico e l'ambito dei rischi operativi.

Le manifestazioni del rischio informatico, infatti, appartengono al più ampio spettro di quelle del rischio operativo. L'identificazione, valutazione/ misurazione, mitigazione e monitoraggio di tale rischio richiedono professionalità specifiche che non risiedono generalmente nella funzione risk management. In ottica di efficienza, sarebbe auspicabile che venisse esplicitamente richiamata l'opportunità di una stretta collaborazione tra le funzioni preposte al governo della variabile informatica (non inquadrate come funzione di controllo di secondo livello e quindi non richiamate nel paragrafo 5 - Cap. 7 Sezione II) e la funzione di risk management/ Operational Risk Management; ad esempio, le attività di raccolta dati di perdita e le valutazioni di scenari di rischio vedono già coinvolta la funzione Operational Risk Management anche con riferimento ai sistemi informativi.

Ad oggi coesistono processi di analisi del rischio informatico nell'ambito della funzione risk management e processi di sicurezza informatica che, nello svolgere una serie di attività tecniche[8], prendono in esame le componenti di rischio.
In particolare, la responsabilità delle attività, così come definite dagli standard di riferimento nella valutazione e mitigazione del rischio informatico, è oggi in carico in una numerosità elevata di banche al Responsabile della Sicurezza Informatica. Appare condivisibile, e dunque da valorizzare nella norma, la creazione di meccanismi di coordinamento tra le due funzioni nel rispetto delle reciproche competenze; la responsabilità della Sicurezza Informatica non trova nell'ambito dell'impianto normativo una chiara collocazione funzionale.

Un primo elemento di contiguità tra le due funzioni è rappresentato dai fattori di rischio connessi alle componenti tecnologiche che devono potersi correlare agli Event Type definiti per il Rischio Operativo anche da Basilea II, con particolare riferimento ai seguenti aspetti: malfunzionamento, incompletezza e non integrazione dei sistemi informativi,

[8] Prendendo a riferimento i più diffusi standard in materia (ISO 27001), le principali attività gestite nell'ambito della Sicurezza Informatica sono le seguenti: identificazione e classificazione delle componenti dell' infrastruttura IT (tecnologiche, di processo e risorse umane) critiche per lo svolgimento del business e delle minacce a esse associate; mappatura dei rischi di riservatezza, integrità e disponibilità; assessment tecnologici della rischiosità; individuazione delle aree da proteggere ulteriormente e degli interventi da predisporre per garantire la sicurezza; identificazione e messa in atto delle soluzioni di mitigazione dei rischi informatici; valutazione del rischio residuo.

attacchi alle componenti del sistema IT, furti e frodi a danno di asset critici, eventi catastrofali.

D'altra parte, le attività tipiche della Sicurezza Informatica richiedono competenze specifiche che non risiedono generalmente nella funzione risk management. È importante dunque assicurare che le competenze di gestione del rischio informatico e di sicurezza delle informazioni definiscano modalità strutturate per interagire con la funzione di risk management, al fine di integrare le valutazioni di carattere tecnologico nel più ampio processo di gestione e analisi del rischio operativo, così come metodologicamente definito da Basilea II e dalle prassi gestionali in campo Operational Risk Management.

Sul fronte delle soluzioni tecniche, come sottolineato dalla norma, è importante che la funzione di sicurezza informatica mantenga indipendenza di giudizio nell'analisi delle variabili che concorrono alla determinazione del rischio informatico. A tal fine, il dialogo fra la sicurezza informatica e la funzione IT dovrebbe essere improntato a favorire la sinergia delle rispettive competenze pur rispettando l'indipendenza nelle valutazioni; le banche caratterizzate da maggiore articolazione organizzativa attuano questo principio collocando la funzione di sicurezza informatica separata dall'IT.

Inoltre, in termini di approccio metodologico per la gestione di tale tipologia di rischio, si evidenzia come sia
complesso ed oneroso, in particolare per le banche di minori dimensioni ma più in generale per ogni tipologia di banca, supportare tali valutazioni per ogni ambito tecnologico con un approccio quantitativo; pertanto, si ritiene utile avallare l'adozione di approcci anche qualitativi che siano in grado di supportare il processo decisionale in merito alle misure di mitigazione del rischio da adottare.

Inoltre, rileva evidenziare come la norma in consultazione ponga grande attenzione al ruolo dell'utente, definito come "la figura aziendale identificata per ciascun sistema che ne assume la generale responsabilità amministrativa in rappresentanza degli utenti, in rapporto con le funzioni preposte allo sviluppo e alla gestione tecnica". L'utente sembrerebbe dunque più vicino a una figura di business – che per molte realtà italiane sarebbe ancora da identificare – piuttosto che a una figura con competenze tecniche; si ritiene opportuno chiarire tale aspetto nella definizione del ruolo. In assenza delle necessarie competenze tecnologiche da parte dell'utente, appare difficile poter dedurre che la responsabilità del rischio associato ai vari ambiti applicativi e tecnologici sia riconducibile esclusivamente a tale figura. È importante e innovativo che sia definito un processo di accettazione del rischio residuo da parte dell'utente in base alle soluzioni identificate dai referenti con competenze di sicurezza informatica e valutate d'intesa con il risk management; tale approccio rappresenterebbe il giusto equilibrio tra il coinvolgimento del business da un lato e delle figure tecniche dall'altro nella corretta valutazione del rischio informatico e delle soluzioni necessarie alla relativa mitigazione.

Preme infine sottolineare la differenza terminologica tra quanto definito nell'ambito delle metodologie di Basilea II e quanto più comunemente previsto nell'ambito informatico. Ad esempio, in ambito di sicurezza informatica viene svolta un'attività tecnica di test e

valutazione dei presidi posti in essere. Tale attività, realizzata attraverso procedure informatiche (penetration test, vulnerability assessment, etc.), permette di supportare l'identificazione delle minacce più che la valutazione del rischio inerente, in ottica risk assessment dell'Operational Risk Management. Si richiede dunque una particolare attenzione nell'uniformare il linguaggio nelle varie porzioni del corpo normativo.

5. Controllo dei sistemi in *cloud computing* (Capitolo 8, Sezione VI, par. 3) vii

Box 5

In considerazione della relativa novità del modello e della limitata esperienza maturata finora nel settore bancario in tale ambito, si sollecitano commenti sul controllo dei sistemi in cloud computing.

Il cloud computing si configura per le banche come un'opportunità di notevole impatto in termini di flessibilità e rapidità operativa, con ambiti di applicazione che si distribuiscono su tutti i livelli concettuali in cui si organizza l'Enterprise Architecture.

Allo scopo di valutare i principali aspetti da tenere in considerazione per realizzare un adeguato presidio dei rischi e delle opportunità collegate al percorso di transizione verso un modello di cloud computing, è importante distinguere rispetto ai diversi approcci, guardando le differenze tra "Public Cloud" e "Private Cloud".

In particolare, i principali aspetti di attenzione fanno riferimento a vincoli e rischi legati all'utilizzo del "Public Cloud", in termini di servizi che è possibile acquistare, anziché al "Private Cloud", per il quale non si evidenziano, nell'impostazione della governance dei sistemi informativi, particolari differenze rispetto alla scelta e alla realizzazione di altre soluzioni tecnologiche.

Si ritiene che l'analisi del "Public Cloud" debba essere realizzata tenendo in considerazione i modelli di servizio che è possibile adottare, valutando le particolarità di ciascun approccio e gli specifici aspetti legati alla gestione dei rapporti con il fornitore, alla sicurezza, alla continuità operativa e non da ultimo alla compliance.

Segue una veloce panoramica dei più diffusi modelli di servizio che rappresentano le principali caratterizzazioni di un modello di Cloud:

- **Infrastructure as a Service (IaaS):** riguarda interventi nell'ambito delle componenti infrastrutturali quali ad esempio i server, il networking o le risorse di storage. In tale situazione particolare attenzione dovrebbe essere dedicata alle modalità di stoccaggio dei dati: il provider mette a disposizione nel cloud un'infrastruttura nella quale gli utilizzatori possono memorizzare i loro dati o applicazioni. In tal caso il fornitore dei servizi detiene la responsabilità del funzionamento della rete, del suo accesso, dell'hardware ecc.

- **Platform as a Service (PaaS):** riguarda interventi nell'ambito delle piattaforme applicative come ad esempio i middleware, i tool di sviluppo o le piattaforme di monitoraggio. Gli aspetti di attenzione concernono principalmente le modalità di trattamento dei dati: il provider di espone e manutiene una piattaforma che viene messa a disposizione dell'utente; a gestire i dati e le applicazioni su tale piattaforma è tuttavia l'utente stesso.

- **Software as a Service (SaaS)**: modello di servizio relativo all'ambito dello strato applicativo relativo alla fruizione di servizi software.

In tale situazione l'utente è soltanto un consumatore nel cloud: non gestisce nulla direttamente, né le applicazioni, né i dati. Ha soltanto a disposizione funzionalità e ha la possibilità di raggiungere servizi applicativi on-demand.

Infine, per quanto riguarda i modelli di "Community Cloud" e di "Hybrid Cloud", l'attenzione agli aspetti di controllo e sicurezza deve essere sviluppata tenendo conto delle modalità con cui si è scelto di combinare le due forme di organizzazione "Public" e "Private". Nello specifico è infatti possibile affermare che la forma "Community" fa riferimento a un approccio molto vicino al "Public", dove però la popolazione degli utenti che lavorano sulla nuvola è limitata a un insieme ben definito di soggetti; "Hybrid" invece è una forma che deriva dalla combinazione di a private e public, dove si ricerca un compromesso ottimale tra logiche pay-per-use e approcci di virtualizzazione dell'infrastruttura interna.

A livello generale le banche hanno un'esperienza consolidata in merito alle attenzioni di sicurezza dei servizi ICT esternalizzati, quali il facility management e full outsourcing, e analogamente per una gestione in "Public Cloud" appare fondamentale definire a livello contrattuale alcuni aspetti:

- livelli di servizio offerti e garantiti;
- disponibilità, riservatezza e integrità dei dati dell'operatività svolta sulle applicazioni da parte della banca;
- trasparenza nelle modalità di trattamento dei dati da parte del Service Provider;
- conoscenza e definizione della localizzazione dei data center e dei dati;
- condivisione di procedure in termini di sicurezza degli accessi e dei log, gestione degli incidenti e continuità operativa
- contesto normativo di riferimento
- verifiche

In prima istanza si evidenzia la buona pratica adottata dalle banche nell'attivare una valutazione attenta in termini di rischi e opportunità delle applicazioni e dei dati che desiderano portare in Public Cloud. Tale attività necessita competenze multidisciplinari che includono usualmente il business, i sistemi informativi, la sicurezza informatica e il legale.

L'elevato livello di standardizzazione dei servizi offerti, necessario per attivare fattori di scala, richiede infatti di incrociare le necessità di sicurezza della banca con le procedure messe in atto da parte del fornitore nella gestione dell'infrastruttura.
In particolare la dinamicità dell'infrastruttura Cloud richiede di elevare il livello di automazione e tempestività delle procedure di sicurezza anche in condivisione con la banca (es. gestione degli incidenti).
Per assicurare questo risulta importante definire contrattualmente le verifiche che la banca ha disponibilità di realizzare eventualmente prevedendo assessment e audit con il fornitore.
Similmente, un altro argomento importante è il controllo dell'attività svolta sugli applicativi e i dati della banca. È quindi necessario approfondire il processo di gestione delle utenze sia della banca che del fornitore nonché la predisposizione e l'analisi di log che permettono il monitoraggio del servizio.

Assumono particolare rilevanza le azioni messe in campo dal fornitore per isolare, segregare gli ambienti, le applicazioni e i dati della banca rispetto alla gestione di altri clienti.

Laddove il fornitore rappresenti una gestione dell'infrastruttura tecnologica e data center al di fuori dei confini nazionali si rileva la necessità di contrattualizzare norme e leggi di riferimento affinché la banca possa ritrovare nell'operatività del fornitore le opportune garanzie rispetto le proprie necessità di compliance (es. Privacy, forum competente).

Un ulteriore tema risulta di essere la conoscenza della localizzazione fisica delle applicazioni e dei dati della banca laddove il fornitore abbia data center al di fuori dell'Italia. Il necessario approfondimento del tema con il fornitore permette di condividere e definire tale localizzazione e la legislazione di riferimento. Si evidenzia peraltro che è opportuno commisurare tale preoccupazione con la criticità del dato in termini normativi e di business e l'economicità di un eventuale gestione specifica per la banca.

Rimangono le attenzioni contrattuali, comuni ai servizi esternalizzati, finalizzate ad evidenziare le modalità di interruzione del servizio per lasciare alla banca la giusta flessibilità nel cambiare fornitore o valutare soluzioni alternative.

In aggiunta i contratti dovranno tenere conto delle garanzie offerte dal Service Provider in merito alla proprietà intellettuale del software della banca.

Commenti particolari

TITOLO V – CAPITOLO 7

IL SISTEMA DEI CONTROLLI INTERNI

SEZIONE I DISPOSIZIONI PRELIMINARI E PRINCIPI DI CARATTERE GENERALE

1. Premessa

2. Fonti normative

3.Definizioni

Il documento sembra non assicurare appieno il principio della neutralità rispetto alle scelte organizzative adottate dalle singole banche, pur nel rispetto degli obblighi posti in termini di assegnazione di responsabilità e di copertura delle funzioni minime, assicurando la corretta separazione tra funzione e unità organizzativa. In particolare, si suggerisce l'inserimento di una definizione relativa al termine "funzione" allo scopo di chiarire che con tale termine non si intende far riferimento a strutture organizzative.
Proposta di inserimento (conseguentemente all'inserimento della lettera e) sottostante, le successive definizioni dalla e) alla g) vengono traslate di una posizione):

"e) "Funzione": insieme di compiti e attività assegnate all'interno dell'azienda allo scopo di assicurarne l'esecuzione. Con tale termine non si intende fare riferimento a specifiche strutture organizzative, esistenti o da costituire".

4. Destinatari della disciplina

5. Unità organizzative responsabili dei procedimenti amministrativi

6. Principi generali

A)

L'ultimo capoverso del paragrafo 6, chiede " alle banche" una verifica annuale del grado di aderenza ai requisiti di controllo interno e dell'organizzazione, La disposizione non è chiara: è sufficiente una delibera che valuti le risultanze delle relazioni delle funzioni di controllo corredata delle relative considerazioni dell'Organo di supervisione strategica? La valutazione dovrà essere svolta dall'Organo con funzione di supervisione strategica, sentito l'Organo con funzione di controllo?

B)

Si richiede una conferma sul fatto che il punto c) di cui al Capitolo 7, Sezione I, par. 6, relativo agli obiettivi dei controlli di conformità, debba essere inteso come conformità alle **norme (esterne) dell'operatività aziendale.** In caso contrario, si genererebbe una

sovrapposizione con la verifica circa la violazione della regolamentazione (interna) attribuita alla funzione di revisione interna. Sarebbe pertanto meglio specificare tale differenza – la stessa osservazione riguarda anche (Capitolo 7, Sezione II, paragrafo 3.4, lettera b).

C)

Al Capitolo 7, Sezione I, par 6 "Principi generali", pag. 6, si stabilisce:

Inoltre, le banche rispettano i seguenti principi generali di organizzazione:
- […];
- *i processi e le **metodologie di valutazione**, anche a fini contabili, delle **attività aziendali** sono affidabili e **integrati con il processo di gestione del rischio**. A tal fine: la definizione e la convalida delle metodologie di valutazione sono affidate a unità differenti; le metodologie di valutazione sono robuste, testate sotto scenari di stress e non fanno affidamento eccessivo su un'unica fonte informativa; la valutazione di uno strumento finanziario è affidata a un'unità indipendente rispetto a quella che negozia detto strumento. […]*

Con riguardo a quest'ultimo alinea, si chiede di voler meglio definire il significato della locuzione "**attività aziendali**", che nelle prime righe sembrerebbe riferirsi ai processi operativi, mentre nelle ultime righe sembrerebbe invece fare riferimento a degli asset. Si chiede inoltre di chiarire le modalità di integrazione dei processi e delle metodologie di valutazione delle stesse con il processo di gestione del rischio. In altre parole, i modelli di valutazione contabili di tipo fair value (sia pure validati dal risk management o dalla convalida interna) e i modelli di valutazione di risk management in senso stretto come possono essere integrati essendo i secondi in genere molto più prudenziali, sia per gli strumenti di trading che di banking book?
Si ritiene, inoltre, che la valutazione in parola debba essere effettuata solo per alcune tipologie di attività particolarmente complesse e dove non esistano riferimenti di mercato puntuali.
Infine, quali sono gli altri fini, oltre a quelli contabili, per cui tali processi e metodologie devono essere utilizzati?

D)

La relazione introduttiva al documento in consultazione indica fra le finalità del complessivo sistema dei controlli interni la «*prevenzione del rischio che la banca sia coinvolta, anche involontariamente, in attività illecite (con particolare riferimento a quelle connesse con il **riciclaggio**, l'usura ed il finanziamento al terrorismo)*» e afferma inoltre che «*Lo schema di disciplina definisce un quadro organico di principi e regole cui deve essere ispirato il sistema dei controlli interni, ma non esaurisce le disposizioni applicabili ai diversi profili operativi delle banche. Esso, piuttosto, rappresenta la cornice di riferimento per le disposizioni sui controlli dettate all'interno di specifici ambiti disciplinari (ad es. in materia di gestione di singoli profili di rischio, di sistemi interni di misurazione dei rischi per il calcolo dei requisiti patrimoniali, di processo ICAAP, di prevenzione del rischio di riciclaggio) che ne completano e integrano la portata*».

Ciò premesso, si chiedono chiarimenti in merito al coordinamento del documento in consultazione con il Provvedimento del 10 marzo 2011 che ha istituito la **funzione antiriciclaggio** in quanto quest'ultimo prevede esplicitamente che la funzione in questione sia una delle funzioni aziendali di controllo anche se lascia alle singole banche la scelta di istituire una funzione aziendale autonoma o di attribuirne i compiti alla funzione di conformità o al risk management.

In base ad una prima chiave di lettura, si potrebbe ritenere che l'assetto organizzativo dei presidi antiriciclaggio sia ancora regolato dal Provvedimento del 10 marzo 2011 (che non viene abrogato) e che quindi le previsioni del documento in consultazione che regolano il funzionamento delle funzioni di controllo non si estendano alla funzione antiriciclaggio che resterebbe regolata dallo specifico provvedimento. Per coerenza si potrebbe concludere che le regole che il documento di consultazione detta per la compliance e per il risk management non si estendano ai compiti antiriciclaggio eventualmente attribuiti alle suddette funzioni dalla banca.

All'opposto si potrebbe sostenere che, dato che il documento in consultazione è una "cornice di riferimento" per le disposizioni sui controlli dettate per specifici ambiti, le previsioni del Provvedimento del 10 marzo 2011 relative alla funzione antiriciclaggio (autonoma o meno) dovranno essere uniformate alle regole generali contenute nel documento in consultazione. Ad esempio, l'obbligo di invio alla Banca d'Italia della relazione annuale delle funzioni di controllo, secondo questa interpretazione si estenderà alla relazione annuale della funzione antiriciclaggio.

* * *

Quesito

Vi deve essere una mappatura dei rischi formalizzata e disponibile alle strutture? Fino a che livello di analiticità devono essere mappati i rischi? In ottica di efficienza dovrebbe essere ammissibile che la fase di identificazione dei rischi sia svolta unitariamente dalle funzioni di controllo di secondo e terzo livello, fatta salva la necessità che le singole funzioni effettuino, ciascuno per quanto di competenza, la valutazione dei rischi mappati.

SEZIONE II

IL RUOLO DEGLI ORGANI AZIENDALI

1. Premessa

2. Organo con funzione di supervisione strategica

Allo scopo di mantenere un'unitaria definizione dei compiti degli organi aziendali, si suggerisce di inserire anche in questo paragrafo le previsioni relative alla continuità operativa. In particolare, si propone di inserire a pagina 9, dopo il punto elenco e) il seguente punto:

f) il piano di continuità operativa; viene informato, con frequenza almeno annuale, sulla adeguatezza dello stesso; stabilisce gli obiettivi e le strategie di continuità del servizio; assicura risorse umane, tecnologiche e finanziarie adeguate per il conseguimento degli obiettivi fissati;

3. Organo con funzione di gestione

A)

Come già espresso nel Box 2, si richiede che venga specificato che il parere preventivo fornito dal Risk Management debba essere incentrato sul profilo di rischiosità complessiva dell'operazione (quindi non vista su un solo rischio ma globale), della sua potenziale redditività (in particolare se trattasi di operazioni complesse sotto il profilo finanziario) ma non ad altri aspetti di competenza di altre funzioni.

B)

Sempre con riguardo **all'organo con funzione di gestione**, si segnala come a questo spetti, secondo il documento (pagg. 11 e 12), di definire il processo diretto alla **distribuzione di nuovi prodotti di investimento** attraverso cui, in particolare, dovrebbero essere definite le fasce di clientela a cui si intendono distribuire nuovi prodotti o servizi in relazione alla complessità degli stessi e ad eventuali vincoli normativi.
Appare opportuno che tale previsione vada quantomeno resa **coerente con quanto previsto dalla vigente regolamentazione CONSOB** in tema di obblighi di valutazione di adeguatezza a carico degli intermediari

C)

Allo scopo di mantenere un'unitaria definizione dei compiti degli organi aziendali, si suggerisce di inserire anche in questo paragrafo le previsioni relative alla continuità operativa. In particolare, si propone di inserire a pagina 12, dopo l'alinea relativo alla definizione della politica aziendale in materia di esternalizzazione, il seguente alinea:

- *promuove lo sviluppo, l'aggiornamento e le verifiche del piano di continuità operativa, garantendo che il tema della continuità operativa sia adeguatamente considerato a tutti i livelli di responsabilità; a tal fine nomina il responsabile del piano di* ***continuità*** ~~*emergenza*~~*; promuove il controllo periodico del piano e l'aggiornamento dello stesso a fronte di rilevanti innovazioni organizzative, tecnologiche e infrastrutturali nonché nel caso di lacune o carenze riscontrate ovvero di nuovi rischi sopravvenuti; approva il piano annuale delle verifiche delle misure di continuità ed esamina i risultati delle prove.*

* * *

Quesito

Al Capitolo 7, Sezione II, par. 3 "Organo con funzione di gestione", pag. 10, si stabilisce:

L'organo con funzione di gestione deve avere la comprensione di tutti i rischi aziendali, inclusi i possibili rischi di malfunzionamento dei sistemi interni di misurazione (c.d. "rischio di modello"), e, nell'ambito di una gestione integrata, delle loro interrelazioni reciproche e con l'evoluzione del contesto esterno.

A questo riguardo si chiede di voler meglio precisare il significato della locuzione "**gestione integrata**" in relazione con il "**principio di proporzionalità**". Ad esempio, si chiede di chiarire se l'approccio "building block", utilizzato per la determinazione del capitale interno complessivo e che esclude le correlazioni tra i rischi, può essere coerente con la gestione integrata dei rischi richiesta.

4. Organo con funzione di controllo

A)

Con riguardo alle funzioni dell'Organismo di Vigilanza (d.lgs n. 231/01) il documento, a p.13, stabilisce che queste siano assegnate alla funzione di controllo, "*salvo che per particolari e motivate esigenze, la banca non decida di affidare tali funzioni a un organismo appositamente istituito*". La disposizione crea ulteriori vincoli organizzativi rispetto a quelli previsti dalla norma primaria (d.lgs 231/01), secondo cui la banca può assegnare sempre, e non solo quando ricorrano particolari e motivate esigenze, le funzioni dell'Odv ad organismo diverso da quello con funzione di controllo.

Si ricorda che la formulazione originaria del d. lgs. n. 231/01 non disponeva dove allocare la funzione svolta dall'Odv, limitandosi a prevedere che l'Odv fosse "*dotato di autonomi poteri di iniziativa e di controllo*". La legge di Stabilità per il 2012 ha correttamente chiarito che la scelta sull'allocazione dell'Odv non può che essere rimessa all'autonomia statutaria delle singole società., dipendendo anche dalla concreta articolazione, nella singola banca, del sistema dei controlli.

Ne consegue che molte banche si sono, legittimamente, determinate verso l'istituzione di un apposito organismo, ritenendolo più funzionale ed altre, altrettanto legittimamente, hanno ritenuto più coerente affidare le funzioni dell'Odv al collegio sindacale o al consiglio di sorveglianza (o ad un comitato costituito al suo interno), in dipendenza del modello di *governance* adottato.

Invece, la disposizione in consultazione riduce eccessivamente la necessaria flessibilità organizzativa in capo all'intermediario: si suggerisce dunque una riformulazione del testo che sia conforme al disposto della norma primaria.

5. Il coordinamento delle funzioni di controllo (interne e societarie)

A)

Con riferimento all'attività dell'Organismo di Vigilanza, il documento la definisce, in questa sezione come attività che attiene in generale all'adempimento di leggi e regolamenti:

la definizione non appare corretta. L'Odv ha il limitato compito di vigilare sul funzionamento e l'osservanza dei modelli di organizzazione e di gestione adottati in tema di responsabilità ex d.lgs. 231/2001, non risultando dunque ad esso attribuiti compiti di controllo di carattere generale.
Si suggerisce dunque di correggere la formulazione.

B)

A mero titolo esemplificativo il documento richiama tra le specifiche funzioni societarie di controllo, la figura dell' "amministratore incaricato del sistema del controllo interno e di gestione dei rischi" prevista dal Codice di autodisciplina delle società quotate (p.14).
Questa figura prevista in via di autoregolamentazione e solo in occasione dell'ultima revisione del Codice di autodisciplina (dicembre 2011),in quanto soggetta, come tutte le altre raccomandazioni del Codice, al principio del *comply or explain*, potra' in concreto non essere attivita presso le singole societa', motivandone le ragioni. La circostanza che il documento di Banca d'Italia richiami tale figura potrebbe ingenerare dubbi sulla natura di questa figura di controllo. Si ritiene dunque opportuno omettere i richiami alle figure di controllo previste dal Codice di Autodisciplina, eliminando il terzo capoverso a p.14.

SEZIONE III

FUNZIONI AZIENDALI DI CONTROLLO

1. Istituzione delle funzioni aziendali di controllo

Si sottolinea l'importanza di distinguere, anche a livello definitorio**, le funzioni di controllo di secondo livello dalla funzione di revisione interna,** che per definizione non esegue attività di controllo in senso stretto, ma appunto attività di revisione (test di funzionalità e conformità).

* * *

Quesito 1

In tema di **nomina e revoca dei Responsabili delle Funzioni di Controllo** il documento a pag. 15 dispone che essi siano nominati e revocati (motivandone le ragioni) dall'organo con funzione di gestione, d'accordo con l'organo con funzione di supervisione strategica, sentito l'organo con funzione di controllo. Il processo descritto sembrerebbe non coerente con quanto previsto nell'ambito delle "Disposizioni sul Governo Societario" (BDI – 04.03.2008) nell'ambito delle quali è previsto che "la nomina del responsabile delle Funzioni di revisione interna e di conformità rientra tra le attribuzioni del CDA non delegabili": ci si chiede se quest'ultima disposizione debba ritenersi abrogata.

Quesito 2 – Declinazione del principio di proporzionalità

Per le banche con approccio di vigilanza *home – host* è importante prevedere la possibilità di mantenere un approccio flessibile sull'assetto organizzativo delle funzioni di controllo, in

coerenza con quello delle banche estere capogruppo, atto a garantire a livello di gruppi internazionali l'omogeneità delle soluzioni organizzative in tema di controlli interni.
Si chiede di valutare se, avuto riguardo all'esigenza di assicurare un rapporto ottimale costi/benefici nell'articolazione e nella conduzione dei controlli, la declinazione del principio di proporzionalità possa prevedere anche la possibilità di non istituire la funzione di revisione interna laddove l'organizzazione dei controlli di 1° e 2° livello e le caratteristiche dell'attività lo consentano per quelle entità che, facendo parte di un Gruppo Bancario, sono comunque soggette / assoggettabili a controlli di revisione interna da parte della Capogruppo sulla base di un sistema di controllo di terzo livello integrato e omogeneo per l'intero Gruppo.
In particolare, si chiede di valutare se una tale previsione possa essere integrata nell'ambito della Sezione V, "Il sistema dei controlli interni nei Gruppi Bancari" individuando **per le controllate vigilate di un Gruppo bancario l**a facoltà di non istituire la funzione di revisione interna laddove l'organizzazione dei controlli di 1° e 2° livello e le caratteristiche dell'attività della controllata nonché l'organizzazione della revisione interna della Capogruppo lo consentano. Ciò comporterebbe infatti il beneficio di un'organizzazione della revisione interna integrata nel Gruppo bancario, la quale utilizzerebbe risorse proprie direttamente presso l'entità sulla base del piano di audit *risk based* (eliminando peraltro gli oneri connessi alla nomina di un referente per l'internal audit interno all'entità del Gruppo). In tal caso verrebbe meno l'applicazione di ogni previsione relativa all'esternalizzazione della funzione di revisione interna per le entità dello stesso Gruppo Bancario.

Quesito 3

Si chiede se la facoltà di conferire la responsabilità di una funzione di controllo ad un componente dell'organo amministrativo privo di deleghe operative sia esperibile in funzione del principio di proporzionalità.

2. Programmazione e rendicontazione dell'attività di controllo

A)

Al Capitolo 7, Sezione III, par. 2 "Programmazione e rendicontazione dell'attività di controllo", pag. 16, si stabilisce:

> *Le funzioni di conformità alle norme e di controllo dei rischi presentano annualmente agli organi aziendali, ciascuna in base alle rispettive competenze, un programma di attività, in cui sono identificati e valutati i principali rischi a cui la banca è esposta e sono programmati i relativi interventi di gestione. La programmazione degli interventi tiene conto sia delle eventuali carenze emerse nei controlli, sia di eventuali nuovi rischi identificati;*

Con riguardo al **programma di attività**, si chiede di voler meglio precisare i criteri che ogni singola banca potrà seguire per identificare il contenuto dello stesso, tenendo in considerazione che le funzioni di conformità alle norme e di controllo dei rischi hanno tra i loro compiti anche attività ulteriori rispetto agli interventi programmati in funzione dell'attività di identificazione e valutazione dei rischi e richiamate, ad esempio, con

riferimento alla funzione di conformità, al paragrafo 3.2 “Funzione di conformità alle norme (compliance)” della Sezione in oggetto.

3. Requisiti specifici delle funzioni aziendali di controllo

3.1 Premessa

Si riportano in premessa alcuni temi più trasversali alle diverse funzioni di controllo. Altre osservazioni nei singoli paragrafi di competenza.

A)

Una delle principali novità del documento, che **si condivide**, è il **rafforzamento** dei poteri della funzione di controllo dei rischi (Risk Management Function - RM).

In linea con questa volontà di rafforzamento si interpreta:

- la previsioni che tale funzione di “*è tenuta a fornire **pareri preventivi** sulla coerenza con la politica aziendale di governo dei rischi delle operazioni di maggiore rilievo*”, previsione che si **condivide** seppure con delle richieste di affinamento (vedi Box 2);
- l’indicazione che “*il responsabile della funzione può essere collocato alle dirette dipendenze del comitato controllo e rischi, ove costituito, o dell’organo con funzione di supervisione strategica*” e la relativa nota (22).

Rispetto a questo secondo bullet, si hanno, invece, le seguenti perplessità:

- quale è la ratio per cui la collocazione “*..alle dirette dipendenze …*” è obbligatoria solo per le banche di classe 1 e 2, in virtù della nota 22?
- il termine “*dirette dipendenze*” deve essere necessariamente inteso in senso gerarchico o in termini di “riferiscono direttamente”? Nella seconda ipotesi, essendo questa previsione già citata (Sezione III paragrafo 1 punto b) quarto alinea) **non si comprende la necessità di specificarla nuovamente.** Nella ipotesi di interpretazione gerarchica, in virtù della nota 22 si riscontrerebbe, invece, una **pesante imposizione organizzativa,** limitata per altro solo alle banche di classe 1 e 2. Pertanto, si chiede di **eliminare la nota 22**, **lasciando quindi che gli intermediari, di qualsiasi classe ICAAP, possano eventualmente autonomamente adottare la soluzione di collocare la funzione Risk management alle dirette dipendenze degli organi citati.** Anzi, proprio tra le banche di classe 3, escluse dalla obbligatorietà per ora imposta dalla nota 22, vi sono realtà che potrebbero adottare una collocazione alle “*dirette dipendenze*” in senso gerarchico. Infatti, nelle ridotte dimensioni la verticalizzazione delle strutture organizzative presenta caratteri più pervasivi rispetto a realtà più articolate che portano ad allocare sostanzialmente parecchi poteri nell’organo di gestione, tipicamente la Direzione generale. Ne discenderebbe che una posizione organizzativa del Risk management alle dipendenze funzionali della Direzione potrebbe concorrere a ridurne le potenzialità anche con riferimento al parere che la funzione è chiamata ad esprimere per le operazioni di maggior rilievo;

- per contro, e a testimonianza della necessità di **rispettare il principio di autonomia organizzativa,** in alcune altre realtà una interpretazione gerarchica del termine "*dirette dipendenze*" potrebbe creare notevoli problemi alla funzione di controllo dei rischi la quale, potendo comunque in virtù delle novità introdotte riferire direttamente agli organi di vertice e formulare pareri preventivi, vedrebbe resa più problematica la restante parte delle proprie attività più direttamente gestionali. Tale previsione di "**allontanamento organizzativo**" rispetto all'attuale collocazione nella struttura operativa potrebbe anche essere vista in contrasto con quanto richiesto nel documento ossia "*individuate soluzioni organizzative che non determinino una eccessiva distanza dal contesto operativo perché per la piena consapevolezza dei rischi è necessario che vi sia una continua interazione critica con le unità di business.*". Questo non vale in assoluto ma rafforza l'ipotesi di lasciare a tutte le banche di qualsiasi classe ICAAP, piena libertà organizzativa;
- da ultimo, si rileva che il documento ricalca per il Risk management i requisiti richiesti per l'Internal Audit, quando invece si tratta di funzioni di livello differente rispondente a diverse esigenze anche organizzative.

In ogni caso, si sottolinea l'importanza di addivenire, pur nel quadro della autonomia organizzativa più volte richiamata, ad una collocazione della funzione di controllo dei rischi che non la renda marginale e al contempo non avulsa dalla realtà gestionale della banca.

B)

Si richiede flessibilità su un aspetto di particolare rilevanza, ossia le soluzioni organizzative che prevedono la figura del *Chief Risk Officer* **(CRO),** inteso come figura di supervisione/coordinamento di **autonome e separate funzioni (i) di controllo dei rischi, (ii) di conformità ed eventualmente (iii) altre funzioni.**

Ovviamente, l'istituzione della figura CRO non è e non dovrà mai essere considerato un obbligo: ciò non di meno, si richiede all'Organo di Vigilanza una valutazione/interpretazione dei possibili ruoli delle diverse funzioni di controllo in presenza di questa nuova figura organizzativa e delle inter-relazioni che ne scaturiscono, le quali si ritiene possano contribuire a delineare l'auspicato percorso di una visione sempre più integrata dei rischi .

In particolare si ritiene opportuno tenere presente la distinzione tra **attribuzioni assegnate alle funzioni** di controllo rispetto alle **soluzioni organizzative** (strutture/unità organizzative) più idonee a consentire un efficace presidio sui rischi.

In questo quadro, considerando anche alcuni recenti riferimenti[9] in materia, si ritiene che la funzione di controllo dei rischi (risk management function) - in relazione alle caratteristiche

[9] Quanto riportato nella nota del Governatore di Banca d'Italia per l'applicazione delle disposizioni di vigilanza in materia di organizzazione e governo societario delle banche, che invitava a porre attenzione sul "corretto ed efficiente funzionamento della funzione di gestione del rischio (risk management) […] nonché sul soggetto responsabile di tale funzione (CRO)". Inoltre, la relazione preliminare che accompagna il documento in consultazione laddove viene citato il CRO nell'ambito della funzione di controllo dei rischi. Infine i contributi sul tema prodotti dalle diverse istituzioni internazionali competenti (es. Principio n°6 di "Principles for enhancing corporate governance" del Comitato di Basilea).

dell'intermediario e a condizione di una piena trasparenza sulle scelte effettuate e nel rispetto degli obiettivi sostanziali della normativa - **possa essere di responsabilità del CRO,** segnatamente anche nei casi in cui al CRO riporti anche un autonomo e separato compliance risk management. Si auspica una esplicita indicazione in tal senso nel documento in consultazione.

C)

Altro aspetto è il seguente. Si chiede che nel documento si faccia riferimento alla possibilità di attribuire la **funzione** di conformità alle norme (compliance) al responsabile **dell'unità** "gestione dei rischi di conformità", **anche qualora tale soggetto riporti gerarchicamente al CRO (**inteso come figura di supervisione/coordinamento di autonome e separate funzioni (i) di controllo dei rischi, (ii) di conformità ed eventualmente (iii) altre funzioni). Ciò purché il responsabile della unità "gestione dei rischi di conformità" mantenga la possibilità, come già avviene sulla base della normativa attualmente vigente, di comunicare agli Organi di Amministrazione e Controllo in via indipendente, mediante invio di flussi informativi e con partecipazione diretta.
Il modello di riferimento delle funzioni aziendali di controllo recepito nel documento in consultazione da Banca d'Italia sembrerebbe invece ispirato alle linee guida EBA in ambito Corporate Governance che prevede l'istituzione di una funzione di controllo dei rischi e di una funzione di conformità alle norme permanenti e indipendenti tra loro, senza alcun punto organizzativo di contatto, ammettendo una deroga nel caso di principio di proporzionalità "*Se coerente con il principio di proporzionalità, le banche possono, a condizione che i controlli sulle diverse tipologie di rischio continuino ad essere efficaci, affidare lo svolgimento della funzione di conformità alle norme alle strutture incaricate della funzione di controllo dei rischi"*.
A tal riguardo sarebbe opportuna una ulteriore riflessione su tale impostazione di modello da parte della Vigilanza tenendo conto che un coordinamento da parte del CRO anche delle attività della funzione di conformità, mantenendo in capo alla stessa un riporto diretto e indipendente agli organi di amministrazione e controllo della Banca e dando pieno riconoscimento delle **proprie peculiarità e specializzazioni**, garantirebbe l'adozione di un approccio più integrato alla gestione dei rischi rispettoso delle loro **interrelazioni reciproche** e dell'evoluzione del contesto esterno, più volte evidenziato dalla normativa stessa (sezione II, par. 3 sul ruolo dell'organo con funzione di gestione; sezione II par. 5 sul coordinamento delle funzioni di controllo interne). Inoltre, la richiesta di parere preventivi al Risk management con riferimento alle operazioni di maggior rilievo (sezione II par. 3) confermerebbe l'esistenza di forti interrelazioni con quanto già richiesto alla funzione di conformità in tema di valutazioni ex-ante della conformità alla regolamentazione applicabile di tutti i progetti innovativi che la banca intende intraprendere e l'opportunità di riconoscere alle banche un grado di maggior flessibilità sulle soluzioni organizzative applicabili a condizione di una piena trasparenza sulle scelte effettuate e nel rispetto degli obiettivi sostanziali della normativa (indipendenza sostanziale delle funzioni di controllo, prevenzione del rischio ed efficienza dei processi aziendali).

3.2 Funzione di conformità alle norme (compliance)

A)

Con riferimento alla disposizione "*Tuttavia, la funzione presiede alla gestione del rischio di non conformità alle norme, con riguardo a tutta l'attività aziendale"* si rileva la portata fortemente innovativa che essa può avere a seconda della interpretazione del termine "**presiedere** alla gestione". Se il **presiedere** comporta una **responsabilità ultima** della funzione di conformità, allora si segnala che **non si concorda** nell'estendere l'attività della funzione di compliance a tutte le normative che hanno impatto aziendale. Tale ipotesi oltre che operativamente non praticabile in molte realtà, soprattutto di minori dimensioni, ed oltre ad essere spesso in contrasto con il principio di economicità[10], intrinsecamente contrasta con la prima parte del paragrafo in quando non renderebbe più necessario non prevedere di fatto un perimetro diretto della funzione.

Invece, confermando anche quanto espresso nel documento "*Riflessioni del Settore Bancario in tema di Perimetro della Funzione Compliance" (Aprile 2008)"* la funzione di conformità dovrebbe avere un perimetro di riferimento obbligatoriamente ricomprendente solo le normative rilevanti e non specialistiche mentre per le altre normative dovrebbe essere **lasciata la facoltà organizzativa alla Banca di decidere se le attività di gestione del rischio di conformità possano essere svolte,** eventualmente con metodologia condivisa, **da altre funzioni** (si veda più avanti punto C una proposta in tal senso del termine "presiedere").

In sostanza, si ritiene che l'area di responsabilità della funzione di conformità, non debba essere **obbligatoriamente allargata,** e a maggior ragione se a **settori specialistici,** a settori la cui attività di per se è connotata dalla ricerca della conformità **o a settori in cui la normativa primaria identifica chiaramente responsabilità specifiche su figure differenti** (Responsabile Sicurezza sul Lavoro, Dirigente Preposto ex art. 154-bis T.U.F., ecc.).

B)

Con riferimento alle principali responsabilità e compiti attribuibili alla funzione di conformità alle norme (compliance) - (cfr. par. 3.2 di pag. 17) - il documento in consultazione precisa che particolare attenzione deve essere posta anche alla verifica della conformità dell'attività aziendale alle **normative di natura fiscale** al fine di evitare di incorrere in violazioni o elusioni di tale normativa ovvero in situazioni di abuso del diritto, che possono determinare ripercussioni significative in termini di rischi operativi e di reputazione e conseguenti danni patrimoniali.

[10] Tra l'altro, nell'indagine sullo stato dell'arte e le prospettive della funzione di compliance nelle banche italiane condotta dall'ABI nel 2011 in collaborazione con lo Studio Limentani & Partners (presentato al convegno ABI Compliance in Banks nel novembre dello scorso anno) ha evidenziato, su un campione di 40 fra banche e gruppi bancari, che nell'86% delle banche di minori dimensioni le risorse dedicate stabilmente alla compliance sono ricomprese tra 1 e 5. La gestione del rischio di non conformità alle norme con riguardo a tutta l'attività aziendale, potrebbe essere svolta con reale efficacia solo con un forte incremento di competenze e risorse, soluzione particolarmente onerosa e di difficile attuazione in particolare ma non solo nelle banche di minori dimensioni.

Premesso che la previsione di un sistema di controllo dell'attività aziendale rispetto alle normative di natura fiscale è un aspetto ormai ineludibile nell'ambito del più ampio tema del sistema dei controlli, in merito alla sua "attribuzione" alla funzione di conformità alle norme, si fa presente, come peraltro ricordato nel documento di consultazione, che è all'esame al Parlamento il disegno di legge delega – atto C. 5291 - in corso di approvazione e recante "Disposizioni per un sistema fiscale più equo, trasparente e orientato alla crescita" nel quale è contemplata, per i soggetti di grandi dimensioni, proprio la previsione di sistemi aziendali strutturati di gestione e di controllo del rischio fiscale, con una chiara attribuzione di responsabilità nel quadro del complessivo sistema dei controlli interni.

In particolare, nella relazione di accompagnamento del provvedimento si precisa che:
- l'intervento normativo trae origine dall'esigenza di favorire nelle imprese la diffusione di modelli della funzione fiscale non più esclusivamente basati sulla "minimizzazione degli oneri fiscali" ma su una vera e propria gestione del rischio di assolvimento degli obblighi fiscali;
- le imprese devono costruire una "mappa" dei rischi relativi all'adempimento degli obblighi tributari, approntare meccanismi di gestione e controllo dei medesimi rischi e definire una chiara attribuzione delle responsabilità, nel quadro del complessivo sistema dei controlli interni e di governance aziendale.

Tenuto conto di quanto sopra e per evitare il rischio che, con la delega in corso di attuazione, gli intermediari finanziari si trovino di fronte a disposizioni di vigilanza non coerenti, in tutto o in parte, con la normativa di attuazione della richiamata legge delega, si propone di attendere il completamento del relativo processo attuativo, considerato anche che i tempi non potranno essere lunghi in ragione dell'approssimarsi della fine della legislatura.

A questo proposito, si sottolinea come le banche, in particolare quelle di maggiori dimensioni, adottino già dei presidi procedurali e organizzativi per la gestione e il controllo del rischio fiscale e in tal senso, siano comunque disponibili a confrontarsi con la Banca d'Italia sui tali presidi, per valutarne la coerenza con le esigenze dell'Organo di Vigilanza.

C)

Interpretazione del termine presiedere e proposta di gamma di ruoli della Funzione di conformità

Per meglio affrontare il tema del processo di gestione del rischio di non conformità in termini di ruoli e responsabilità appare utile prefigurare tre fasi:

a) **disegno** del framework di gestione del rischio di non conformità **per una determinata area normativa;**

b) **attuazione** del framework di cui sopra;

c) definizione di una **visione integrata** sulle diverse aree normative che si applicano alla banca.

Disegnare il framework di gestione del rischio di con conformità relativo ad una determinata area normativa significa disegnare «*l'insieme delle regole, delle procedure e delle risorse volte a identificare, misurare o valutare, monitorare, attenuare*» di non conformità (definizione di *Processo di gestione dei rischi pag. 3 punto g).*

Una funzione responsabile di **disegnare** tale framework (azione una tantum) e di verificarne periodicamente la tenuta complessiva **può essere una funzione diversa** da quella che ha la responsabilità di **attuarlo** ossia nel continuo e nel concreto identificare, misurare o valutare, monitorare, attenuare il rischio di non conformità.

La fase c) spetta sempre alla funzione di conformità (**FC**).

La FC può essere responsabile del disegno di un dato framework e poi di attuarlo (è il caso tipico e certamente presente per molte delle norme chiamate "rilevanti" nel documento in consultazione) ma si ritiene che la FC possa anche:

- **essere responsabile del disegno** un framework la cui responsabilità di attuazione spetta ad altri;
- **essere solo di supporto** ad una altra funzione (che poi attua il framework) nella fase di disegno del framework stesso.

Questi due casi potrebbero essere adeguatamente utilizzati, ad esempio, per una area normativa sulla quale la **funzione specialistica** (FS) - od una specifica struttura organizzativa - ha già un responsabilità operativa. In particolare il secondo bullet del paragrafo precedente richiama in qualche misura la parte del documento in consultazione in cui si cita **l'ausilio che la FC deve fornire ad altre strutture aziendali** con riferimento a fasi del processo di gestione del rischio di non conformità (cfr. Capitolo 7, Sezione III, par. 3 "Funzione di conformità alle norme (compliance)", pag. 18, per quanto concerne gli adempimenti della FC).

In tale quadro, da un punto di vista di idonea attribuzione di compiti e responsabilità, si sottolinea che **se la FC ha disegnato in modo corretto il framework** e ne ha valutato periodicamente la efficacia, in presenza di problemi derivanti dalla non corretta applicazione del framework, la FC non può esserne considerata responsabile. Ciò vale anche nel caso in cui la FC abbia supportato altri nel disegno del framework.

Quindi nel rispetto della autonomia organizzativa**, il ruolo e la responsabilità** della FC che il **termine "presiede"** genericamente richiama, **devono essere chiariti.**

Per quanto sopra detto il ruolo e la responsabilità della FC possono essere, **per alcune aree normative, circoscritti al disegno del framework** di gestione del rischio di non conformità**, al supporto** fornito alla FS **nel disegno del framework** ed**,** infine**,** eventualmente al **monitoraggio della tenuta.** E' questa una declinazione certamente meno pervasiva e operativamente più accettabile del termine "presiede". In ogni caso la **visione unitaria** della esposizione al rischio di non conformità **verrà fornita dalla FC** agli organi di vertice.

L'approccio, comunque finalizzato ad una corretta gestione dei rischi, anche di tipo reputazionale, è volto ad evitare che alla FC siano attribuite responsabilità dirette su ambiti

che richiederebbero duplicazioni di competenze e strutture. Più in generale, si osserva che quest'ultimo aspetto è ampiamente evidenziato anche al paragrafo 5 sul coordinamento delle funzioni di controllo interne ed esterne (sezione II, par.5)… "*Il corretto funzionamento del sistema dei controlli interni si basa sulla proficua interazione nell'esercizio dei compiti fra gli organi aziendali, gli eventuali comitati all'interno di questi ultimi, i soggetti incaricati della revisione legale dei conti e le funzioni aziendali di controllo (compliance, risk management, internal audit). Per assicurare una corretta interazione tra tutte le funzioni e organi con compiti di controllo, evitando sovrapposizioni e lacune, l'organo con funzione di supervisione strategica approva un documento nel quale sono definiti i compiti e le responsabilità dei vari organi e funzioni (aziendali e societarie) di controllo, i flussi informativi tra le diverse funzioni e tra queste e gli organi aziendali e le modalità di coordinamento e collaborazione"*… e poi nel paragrafo 3.5 della sezione III in tema di rapporti tra le funzioni aziendali di controllo e altre funzioni aziendali "*Fermo restando la reciproca indipendenza e i rispettivi ruoli, le funzioni aziendali di controllo collaborano tra loro e con le altre funzioni (es. legale, organizzazione, sicurezza informatica) allo scopo di sviluppare le proprie metodologie di controllo in modo coerente con le strategie e l'operatività aziendale"*…

D)

L'impostazione illustrata la punto precedente ben si presta, ad esempio, ai complessi processi di **Vigilanza Prudenziale,** ossia ad una area normativa di tipo particolare, il cui rispetto è insito nella gestione del rischio che la stessa declina.
Pertanto, anche alla luce di alcuni provvedimenti sanzionatori dell'Autorità di Vigilanza e di uno **studio specifico** in via di completamento in sede **ABICS** su FC e Vigilanza Prudenziale, il documento di Banca d'Italia in consultazione dovrebbe meglio chiarire la possibile suddivisione dei ruoli tra funzione di compliance e altre funzioni specialistiche coinvolte nei processi di Vigilanza Prudenziale (fatta eccezione per quanto esplicitamente attribuito alla **funzione di convalida** per le banche adoperanti sistemi avanzati per la determinazione dei requisiti minimi patrimoniali).

In ottica di efficacia ed efficienza, visto il *know how* necessario, nonché in linea con il principio di proporzionalità, **si chiede di esplicitare che la Vigilanza Prudenziale** - pur rientrando da un punto di vista definitorio nel novero delle norme che regolano l'esercizio dell'attività bancaria e di intermediazione **- ha caratteristiche tali per cui è lasciata agli intermediari autonomia in materia di connesse scelte organizzative.**

Tali scelte potrebbero spaziare:

- dalla inclusione nel perimetro della funzione di conformità di alcuni fra i processi di Vigilanza Prudenziale (responsabilità della funzione in tutte e tre le fasi di cui al precedente punto C);
- alle altre combinazioni possibili relativamente alla fase a) del disegno e alla b) della attuazione.

Ad esempio alle **funzione specialistiche** (es. risk management ma anche funzioni non di controllo) potrebbe andare la responsabilità di **attuare tale *framework*** (ossia la concreta opera di identificazione, valutazione/misurazione, monitoraggio ed attenuazione) ma

secondo un **disegno definito dalla funzione di conformità** e approvato dagli organi aziendali.

E)

Si auspica che, nella versione definitiva della normativa, sia esplicitata la possibilità di ricorre ad **Accordi di Servizio**.

Si ricorda a tal riguardo il lavoro pubblicato su Bancaria n. 2/2011 sugli “Accordi di Servizio (AdS) tra Funzione Compliance e l’Interal Auditing” in quanto essi possono rappresentare una opzione efficace ed efficiente al perseguimento degli obiettivi assegnati alla Funzione e più in generale al complessivo sistema dei controlli aziendali.

Si ricorda che gli AdS possono essere delle valide soluzioni anche nel caso in cui il “committente” è costituito dall’Internal Auditing e non solo viceversa.

Sarebbe importante quindi inserire un riferimento a tale opzione gestionale nelle parti del documento afferenti sia nel piano di auditing che in quello della compliance, oppure nel paragrafo dedicato ai rapporti tra le funzioni di controllo.

F)

In merito alle **verifiche** richieste dalle Autorità di Vigilanza come **attività straordinaria e una tantum**, si chiede di esplicitare che tali evenienze non impongano, nelle fasi successive, una collocazione nell’area di responsabilità della FC delle norme o dei processi coinvolti.

G)

Alla luce del divieto per i responsabili delle funzioni di controllo di avere responsabilità diretta di funzioni operative sottoposte a controllo, si chiede di confermare che la struttura che gestisce i reclami non debba essere considerata una struttura operativa dell'intermediario e possa pertanto dipendere gerarchicamente dal responsabile della funzione di compliance. Al riguardo si cita l'art. 16 del Regolamento congiunto Banca d'Italia-Consob del 29 ottobre 2007 che prevede che le relazioni presentate dalla funzione di Compliance riportino "*la situazione complessiva dei reclami ricevuti, sulla base dei dati forniti dalla funzione incaricata di trattarli, qualora differente dalla funzione di controllo di conformità*". Quanto sopra, non si porrebbe in contraddizione con la facoltà per l'intermediario di disporre di una struttura di gestione dei reclami che riporti gerarchicamente al Responsabile della funzione di compliance.

Alcune banche includono nelle attività della Funzione Compliance il monitoraggio (censimento, rispetto dei tempi di risposta, ecc.), l’analisi e le conseguenti azioni relative a tutti i reclami, ivi compresi i reclami non Mifid (cosiddetti bancari). Premesso che la Funzione debba avere libero accesso al registro dei reclami (se non gestito direttamente) l’attività di vera e propria trattazione dei reclami è stata in altri casi esclusa dal perimetro, mentre rimaneva incluso il monitoraggio di tutti i reclami. La trattazione del reclamo implica, infatti, una transazione da parte della banca. Poiché in talune interpretazioni tali

transazioni particolari con il cliente vengono interpretate come espressione di una funzione operativa non propria dalla Funzione Compliance, il non includere la trattazione dei reclami nel perimetro di competenza potrebbe eventualmente essere l'unica limitazione imposta.

* * *

Quesiti

1)
Il documento in consultazione mantiene la previsione contenuta già nella comunicazione del 2007 in base alla quale «*In relazione ai molteplici profili professionali richiesti per l'espletamento di tali adempimenti, le varie fasi in cui si articola l'attività della funzione di conformità alle norme possono essere affidate a strutture organizzative (es. legale, organizzazione, gestione del rischio operativo), purché il processo di gestione del rischio e l'operatività della funzione siano ricondotti ad unità mediante la nomina di un responsabile che coordini e sovrintenda alle diverse attività.*».
Si chiede se in questo concetto rientri anche la possibilità per la compliance di avvalersi di **risorse e funzionalità dell'internal audit** per l'effettuazione di **verifiche in loco**, facoltà espressamente prevista dalla Comunicazione congiunta Banca d'Italia – Consob dell'8 marzo 2011 in materia di ripartizione dei compiti fra Compliance e Internal Audit nella prestazione dei servizi di investimento.

2)
Si chiede, altresì, se sia possibile avvalersi di **professionisti esterni**, esternalizzando di fatto la gestione del rischio di non conformità con riferimento alla generalità dei rischi di competenza della compliance e in particolare alla **normativa fiscale**.

3.3 Funzione di controllo dei rischi (risk management function)

Con l'obiettivo di convenire sulla opportunità di rivedere alcune parti del documento che non appaiono in linea con il principio di preservazione dell'autonomia organizzativa, nel quadro di quanto già esplicitato ai punti A), B), C) della premessa (punto 3.1), si riportano nel seguito alcuni aspetti che riflettono soluzioni peculiari già implementate e in via di definizione presso gli Associati meritevoli di approfondimento.

A)

Al fine di rafforzarne l'indipendenza, il responsabile della funzione di controllo dei rischi puo' essere collocato alle dirette dipendenze del comitato controllo e rischi, ove costituito, o dell'organo con funzione di supervisione strategica. Viene poi espressamente richiesto nella nota 22 di pagina 19, *nel caso di Banche classificate ai fini SREP nelle macro-categorie 1 e 2 un suo collocamento obbligatorio alle dirette dipendenze del comitato controllo e rischi, ove costituito o dell'organo con funzione di supervisione strategica.*
In tema di partecipazione della funzione ai comitati di gestione dei diversi profili di rischio (ad es. comitati per i rischi di credito e operativi, comitato di liquidità, ecc..) viene chiesto di *"…definire in modo chiaro le diverse responsabilità e le modalità di intervento e di partecipazione della funzione in modo da garantirne la completa indipendenza dal processo*

di assunzione dei rischi; va inoltre evitato che l'istituzione di tali comitati possa depotenziare le prerogative della funzione di controllo dei rischi.
Al tempo stesso, vanno individuate soluzioni organizzative che non determino una eccessiva distanza dal contesto operativo. Per la piena consapevolezza dei rischi è necessario che vi sia una continua interazione critica con le unità di business.

Osservazioni, commenti e proposte:

Come caso peculiare di quanto già esposto al punto A) della sezione "3.3.1 Premessa" per quanto concerne la **collocazione organizzativa del responsabile della funzione di controllo dei rischi (nel caso specifico attribuita al CRO)**, richiamata nel documento in consultazione, alla **nota 22** che prevederebbe il CRO alle dirette dipendenze del Comitato Controllo e Rischi ove costituito (Comitato interno al Consiglio di Amministrazione che svolge sia funzioni di supervisione strategica che di gestione nel caso di modello di amministrazione e controllo tradizionale; nel caso del modello dualistico, Comitato Controllo Interno, costituito in seno al Consiglio di Sorveglianza che assume sia funzioni di supervisione strategica che di controllo), o dell'Organo con Funzione di Supervisione Strategica (nella medesima formulazione utilizzata poi anche per la funzione di revisione interna per tutte le banche a prescindere dalla loro classificazione ai fini SREP nelle macro-categorie 1 e 2) **si ritiene che la formulazione della nota possa risultare incoerente rispetto dei seguenti assunti richiesti dalla normativa stessa:**

1) che siano "*individuate soluzioni organizzative che non determinino una eccessiva distanza dal contesto operativo perché per la piena consapevolezza dei rischi è necessario che vi sia una continua interazione critica con le unità di business"* e
2) che l'organo con funzione di gestione (es. Consiglio di Gestione) "*esamina le operazioni di maggior rilievo oggetto di parere negativo da parte della funzione di controllo dei rischi e se del caso le autorizza: di tali operazioni informa l'organo con funzione di supervisione strategica e l'organo con funzione di controllo*" …che confermerebbe la partecipazione nel continuo da parte del CRO alle attività con un ruolo tecnico-consultivo e la presenza di successivi flussi informativi regolari all'organo con funzione di supervisione strategica e di controllo (es. Consiglio di Sorveglianza).

Tenendo fermo il principio di distinzione tra funzione e unità/struttura organizzativa, anche l'attribuzione della funzione di gestione dei rischi al Chief Risk Officer non pone vincoli di carattere organizzativo, anche qualora questi riporti gerarchicamente al Chief Executive Officer (CEO, Consigliere Delegato, responsabile di promuovere il presidio integrato dei rischi), e sia formalizzato che il responsabile di detta funzione mantenga la possibilità di comunicare agli organi di Amministrazione e Controllo in via indipendente, mediante invio di flussi informativi e con partecipazione diretta, sia in maniera regolare che su richiesta.
Questa interpretazione inoltre, renderebbe più evidente il peculiare ruolo della funzione di terzo livello (Audit) che riporterebbe essa unicamente direttamente all'organo con funzione di supervisione strategica e di controllo (es. Consiglio di Sorveglianza) e la funzione di controllo di secondo livello (CRO) in riporto gerarchico al CEO, evitando quindi possibili duplicazioni e sovrapposizioni di ruolo tra le due.
Ad ulteriore evidenza del grado di indipendenza del CRO rispetto al CEO sono le procedure di nomina/revoca e di remunerazione dei responsabili delle funzioni di controllo e quindi

anche del CRO che non rientrano nelle autonome attribuzioni del CEO ma di comitati indipendenti costituiti in seno al Consiglio di Sorveglianza.
Da ultimo si consideri che tale interpretazione, non irrigidirebbe le modalità di funzionamento degli organi aziendali e delle funzioni di controllo interne e societarie previsti dalla nuova disciplina (Capitolo 7-Sezione II), attenuando il rischio di applicazioni nel caso concreto, molto onerose ed eterogenee ad esempio tra banche che adottano un sistema di amministrazione e controllo di tipo dualistico anziché tradizionale (basato sul Consiglio di Amministrazione e Collegio Sindacale e ispiratore del modello di corporate governante delineato nel Codice di Autodisciplina a cui il documento in consultazione si ispira) che di fatto potrebbero dimostrarsi formalmente rispettose delle previsioni normative ma meno efficaci nell'applicazione dei principi generali alla base della disciplina che mirerebbe a promuovere il rafforzamento della capacità di gestire e prevenire i rischi a rinforzo della sana e prudente gestione delle banche e della stabilità del sistema finanziario.
Anche in relazione a quanto sopra riferito si auspica quantomeno una riformulazione della nota 22 di pag. 19.

B)

Il documento in consultazione (punti 3.3 e 3.4) prevede il collocamento della funzione di controllo dei rischi (e della funzione di revisione interna) alle dirette dipendenze del comitato controllo e rischi, ove costituito, o dell'organo con funzione di supervisione strategica.
Al riguardo si richiede di chiarire se nel **modello dualistico**, quando il consiglio di sorveglianza abbia per volontà dello statuto funzioni di supervisione strategica, la collocazione delle funzioni di controllo alle dirette dipendenze del comitato controllo e rischi possa comportare il trasferimento della funzione di vigilanza, e della conseguente responsabilità, dal plenum (così come oggi attribuita) al comitato, al quale attualmente sono attribuiti esclusivamente compiti propositivi, consultivi e istruttori relativi all'esercizio della funzione di vigilanza spettante in via originaria ed esclusiva al consiglio di sorveglianza.
Il documento in consultazione non consente di evincere se la collocazione delle funzioni di controllo alle dirette dipendenze del comitato controllo e rischi abbia carattere opzionale (nel senso che il consiglio di sorveglianza potrebbe anche decidere di collocare tali funzioni direttamente alle proprie dipendenze), oppure obbligatorio.

3.4 Funzione di revisione interna (internal audit)

A)

"..verifica, anche attraverso accertamenti di natura ispettiva:
a) la regolarità delle diverse attività aziendali, incluse quelle esternalizzate, e l'evoluzione dei rischi sia nella direzione generale della banca, sia nelle filiali. La frequenza delle ispezioni deve essere coerente con l'attività svolta;..."

Si richiede di chiarire se la verifica sulle **attività esternalizzate** debba intendersi come analisi direttamente svolta dalla funzione di Revisione Interna su tutti i processi in

outsourcing o può prendere a riferimento le verifiche svolte anche da altre strutture aziendali per il controllo dello svolgimento delle stesse, ove tali strutture esistano.
Tale seconda ipotesi risulterebbe coerente con la definizione di un piano di audit che preveda lo svolgimento di attività di controllo su significative aree esternalizzate.

"*espleta compiti d'accertamento anche con riguardo a specifiche irregolarità, ove richiesto dagli organi aziendali*"

Il punto relativo agli accertamenti con riguardo a specifiche irregolarità deve poter essere espletato con indipendenza e non "ove richiesto dagli organi aziendali".

Gli esiti degli accertamenti conclusisi con giudizi negativi o che evidenzino carenze di rilievo devono essere trasmessi integralmente, tempestivamente e direttamente agli organi aziendali.

Si suggerisce di eliminare "di rilievo" riferito solo alle carenze e di inserire all'inizio della frase "nel caso di rischi rilevanti".

B)

"...Per svolgere adeguatamente i propri compiti, la funzione di revisione interna deve avere accesso a tutte le attività, comprese quelle esternalizzate, della banca svolte sia presso gli uffici centrali sia presso le strutture periferiche. In caso di attribuzione a soggetti terzi di attività rilevanti per il funzionamento del sistema dei controlli interni (ad esempio, dell'attività di elaborazione dei dati), la funzione di Revisione Interna deve poter accedere anche alle attività svolte da tali soggetti)..."

Si richiedono chiarimenti/esempi circa la **definizione di attività rilevanti** o indicazioni su quale debba essere l'organo/funzione aziendale deputato alla definizione e/o alla approvazione di tali attività. Si richiede inoltre se per la definizione di tali attività debbano essere presi a riferimento i parametri indicati nella definizione di "Funzione operativa importante".

C)

Allo scopo di assicurare l'omogeneità dei termini utilizzati con riferimento alla continuità operativa, si propone di adottare sempre le diciture "piano di continuità operativa" anziché "piano di emergenza". Si suggerisce di modificare pertanto il sesto alinea come segue:

- *controlla regolarmente il piano aziendale di continuità operativa. In tale ambito, prende visione dei programmi di verifica, assiste alle prove e ne controlla i risultati, propone modifiche al piano sulla base delle mancanze riscontrate. La funzione di revisione interna è coinvolta nel controllo dei piani di* ***continuità operativa*** ~~*emergenza*~~ *degli outsourcer e dei fornitori critici; essa può decidere di fare affidamento sulle strutture di questi ultimi se ritenute professionali e indipendenti quanto ai risultati dei controlli ed esamina i contratti per accertare che il livello di tutela sia adeguato agli obiettivi e agli standard aziendali;*

D)

"valuta la conformità dell'operatività aziendale al livello di tolleranza al rischio/appetito per il rischio approvato dall'organo con funzione di supervisione strategica e, in caso di strutture finanziarie particolarmente complesse, la conformità di queste alle strategie approvate dagli organi aziendali".
Si segnala la opportunità di ben distinguere, in tema di risk appetite/tolerance, il ruolo della funzione di controllo dei rischi - che propone e supporta le decisioni degli organi di vertice in merito alle scelta in materia di risk appetite e di conseguente declinazione di risk tolerance - da quello attribuito alla funzione di revisione interna di cui sopra.

3.5 Rapporti tra le funzioni aziendali di controllo e altre funzioni aziendali

Fermo restando che le proposte di Banca d'Italia al riguardo sono, in linea di massima, condivisibili, si evidenzia, ai fini di fornire un utile contributo, come sul tema ABI, insieme a FEDERCASSE ed ASSOISM abbia, nel 2010, elaborato delle Linee guida in tema di rapporti tra funzioni di controllo interno e le altre funzioni aziendali.

SEZIONE IV

ESTERNALIZZAZIONE DI FUNZIONI AZIENDALI (*OUTSOURCING*)

Allo scopo di favorire le operazioni di razionalizzazione delle attività all'interno dei gruppi bancari tramite l'allocazione delle attività presso i diversi soggetti, si propone di specificare **che le disposizioni contenute nella presente Sezione non si applicano ai casi di esternalizzazione infragruppo.**

1. Principi generali e requisiti particolari

A)
Le banche che intendono esternalizzare, in tutto o in parte, lo svolgimento di funzioni operative importanti o di controllo sono tenute a informare preventivamente la Banca d'Italia, fornendo tutte le indicazioni utili a verificare il rispetto dei criteri sopra indicati. Nel caso di esternalizzazioni presso soggetti con sede in altri paesi la comunicazione alla Banca d'Italia deve essere effettuata almeno 30 giorni prima di conferire l'incarico, specificando le esigenze aziendali che hanno determinato la scelta. Entro 30 giorni dal ricevimento della comunicazione la Banca d'Italia può avviare un procedimento amministrativo d'ufficio di divieto dell'esternalizzazione che si conclude entro 60 giorni.

Il processo di comunicazione alla Banca d'Italia relativamente all'esternalizzazione totale o parziale dello svolgimento di funzioni operative "importanti" è alquanto restrittivo e renderebbe opportuna una ridefinizione:

- dell'ambito delle funzioni operative limitandole alle sole "essenziali" in coerenza con quanto già previsto da Consob e da precedenti disposizioni di Banca d'Italia (ad es. esternalizzazione del trattamento del contante);
- del perimetro territoriale sottoposto all'autorizzazione preventiva con una specifica esimente per tutti i soggetti operanti in ambito UE;
- dei tempi complessivi per il procedimento amministrativo di divieto all'esternalizzazione;
- della introduzione delle motivazioni che portano all'eventuale provvedimento di divieto.

B)

Si ritiene opportuno prevedere che la politica aziendale in materia di esternalizzazione contempli anche le tematiche di continuità operativa. La proposta è di integrare il primo alinea come segue:

- *il processo decisionale per esternalizzare funzioni aziendali (livelli decisionali; funzioni coinvolte; valutazione dei rischi, inclusi quelli connessi con potenziali conflitti di interesse dell'outsourcer, e l'impatto sulle funzioni aziendali;* ***valutazione dell'impatto in termini di continuità operativa;*** *criteri per la scelta e la due diligence del fornitore);*

C)

Allo scopo di assicurare l'omogeneità dei termini utilizzati con riferimento alla continuità operativa, si propone di adottare sempre le diciture "piano di continuità operativa" anziché "piano di emergenza" e "procedure di continuità" anziché "procedure di emergenza".

D)

Condividendo gran parte dei principi indicati nella Sezione IV (da pagina 23 del documento) si richiede di modificare la Sezione V (pagina 28) relativa al sistema dei controlli interni nei gruppi bancari in quanto attualmente è più complessa o sottoposta a maggiori valutazioni l'esternalizzazione delle funzioni di controllo presso la capogruppo che l'esternalizzazione verso terzi.

In linea con il principio di proporzionalità si propone che le banche appartenenti alla/e categorie di minori dimensioni/sofisticazione individuino il "referente per le attività esternalizzate" limitatamente alle sole "funzioni operative importanti".

2. Esternalizzazione del trattamento del contante

A)

Si richiede se nel caso in cui le attività di audit su processi in outsourcing vengano svolte dalla funzione di audit del gruppo ma non direttamente dalla funzione internal audit locale, possano essere prese in considerazione le risultanze delle verifiche condotte dalle funzioni

internal audit di gruppo ai fini della stesura della nuova relazione annuale sulle attività esternalizzate anche se non incluse nel piano di audit locale.

SEZIONE V

IL SISTEMA DEI CONTROLLI INTERNI NEI GRUPPI BANCARI

1. Ruolo della capogruppo

Con riferimento alla disposizione secondo cui: "*all'interno di tutte le banche del gruppo e delle altre entità che, a giudizio della capogruppo, assumono rischi considerati rilevanti per il gruppo nel suo complesso vengono individuati appositi referenti i quali: svolgono compiti di supporto per la funzione aziendale di controllo esternalizzata; riportano funzionalmente e gerarchicamente a quest'ultima; provvedono tempestivamente a segnalare eventi o situazioni particolari, suscettibili di modificare i rischi generati dalla controllata"* si osserva che:
- la dipendenza gerarchica tra risorse e strutture appartenenti a diverse società del Gruppo è di difficile applicabilità e rappresenta un elemento di criticità nell'organizzazione delle entità coinvolte.
- essa può inoltre confliggere con l'attribuzione di ulteriori ruoli e responsabilità a detto referente in seno all'attività interessata e quindi con l'indipendenza e obiettività della funzione di revisione interna rispetto alle ulteriori attività svolte da detto referente.
Si ritiene pertanto maggiormente efficiente per gruppi bancari di piccole e medie dimensioni, anche in virtù del principio di **proporzionalità**, di eliminare la previsione riferita al **rapporto gerarchico**.

2. Controlli interni di gruppo

Vedasi anche quanto già espresso al primo capoverso del punto C) del paragrafo precedente.

A)

Con riferimento a quanto previsto dalla Sezione V "Il sistema dei controlli interni nei gruppi bancari", paragrafo 2:

"(…) qualora l'esternalizzazione sia effettuata alla capogruppo, all'interno della funzione di revisione interna della stessa viene mantenuta un'adeguata separazione tra le unità e le risorse deputate a svolgere l'internal audit su base individuale per le controllate da quelle responsabili dei controlli su base consolidata le quali, tra i diversi compiti, hanno anche quello di verificare la funzionalità del complessivo sistema dei controlli interni di gruppo (…)"

Se tale previsione presuppone l'obbligo da parte della funzione di revisione interna della capogruppo di istituire e formalizzare una autonoma unità deputata ai controlli su base consolidata, completamente separata da quella che si occupa dei controlli su base individuale per le controllate, si ritiene che tale previsione:

- non sia in linea con il principio di **economicità** e di **proporzionalità**, in particolare ma non solo per i conglomerati di contenute dimensioni;
- non sia adeguatamente giustificata come limitata alla sola revisione interna e non anche alle altre funzioni di controllo.

Si richiede quindi l'eliminazione del disposto che prevede l'istituzione di una unità di revisione interna deputata ad effettuare in via esclusiva controlli su base individuale. Tra l'altro il criterio prevalente di specializzazione delle risorse di auditing è per ambito/processo e tale impostazione garantisce efficacia ed efficienza certamente maggiore di quella per singola entità o per capogruppo vs entità controllate.

B)

Per le banche italiane controllate da Gruppi internazionali la cui controllante si trovi in altro paese UE, possono esserci funzioni o attività importanti esternalizzate presso la capogruppo estera. Nella realtà dei fatti ci si trova, quasi sempre, di fronte ad una "internalizzazione" di alcune funzioni chiave (ad esempio i modelli interni per la quantificazione dei rischi Basilea II – 2° pilastro, oppure determinate attività di Risk management) che non vengono "delegate" alle società controllate.
Tali attività restano centralizzate presso la controllante estera.

Risulta, conseguentemente, difficile qualificare queste situazioni come "esternalizzazione di attività", trattandosi di fatto di attività o funzioni non delegate.

C)

Il documento di consultazione stabilisce che: "al fine di assicurare l'effettività e l'integrazione dei controlli, l'esternalizzazione delle funzioni aziendali di controllo presso la capogruppo o le altre componenti del gruppo è consentita indipendentemente dalle dimensioni e dalla complessità operativa a condizione che i gruppi bancari si attengano, in aggiunta a quanto previsto dalla Sezione IV, ai seguenti criteri:

- *all'interno di tutte le banche del gruppo e delle altre entità che, a giudizio della capogruppo, assumono rischi considerati rilevanti per il gruppo nel suo complesso vengono individuati appositi referenti i quali: svolgono* ***compiti di supporto*** *per la funzione aziendale di controllo esternalizzata;* ***riportano funzionalmente e gerarchicamente*** *a quest'ultima; provvedono tempestivamente a segnalare eventi o situazioni particolari, suscettibili di modificare i rischi generati dalla controllata.*

La previsione di un riporto funzionale e gerarchico del referente della funzione di revisione interna esternalizzata alla stessa funzione può confliggere con l'attribuzione di ulteriori ruoli e responsabilità a detto referente in seno all'entità interessata e quindi con l'indipendenza e obiettività della funzione di revisione interna rispetto alle ulteriori attività svolte da detto referente. Tale previsione appare peraltro anche difficilmente coordinabile con quella indicata nella sez. IV (esternalizzazione di funzioni aziendali (outsourcing), paragrafo 1 "principi generali e requisiti particolari"[11] che obbliga la funzione di revisione

[11] "Le banche di dimensioni contenute o caratterizzate da una limitata complessità operativa che intendono affidare a soggetti terzi, in tutto o in parte, le funzioni aziendali di controllo definiscono nell'accordo di esternalizzazione, le

interna a dare riscontro tempestivamente a qualsiasi richiesta di informazioni e consulenza da parte del referente per l'attività esternalizzata (oltre che degli organi aziendali).

Si propone dunque di eliminare la specifica previsione riferita al riporto gerarchico ("*riportano funzionalmente e gerarchicamente a quest'ultima*"), eventualmente specificando ulteriori meccanismi atti a preservare la costante integrazione della funzione di revisione interna esternalizzata nell'entità, quali l'obbligo di prevedere costanti flussi informativi.

* * *

Quesito 1
Il documento in consultazione mantiene la previsione contenuta già nella comunicazione del 2007 in base alla quale «*In relazione ai molteplici profili professionali richiesti per l'espletamento di tali adempimenti, le varie fasi in cui si articola l'attività della funzione di conformità alle norme possono essere affidate a strutture organizzative (es. legale, organizzazione, gestione del rischio operativo), purché il processo di gestione del rischio e l'operatività della funzione siano ricondotti ad unità mediante la nomina di un responsabile che coordini e sovrintenda alle diverse attività*».
Si chiede se in questo concetto rientri anche la possibilità per la compliance di avvalersi di risorse e funzionalità dell'internal audit per l'effettuazione di verifiche in loco, facoltà espressamente prevista dalla Comunicazione congiunta Banca d'Italia – Consob dell'8 marzo 2011 in materia di ripartizione dei compiti fra Compliance e Internal Audit nella prestazione dei servizi di investimento.

Quesito 2
Ci si chiede inoltre se referenti all'interno delle Controllate debbano essere dipendenti o possano essere soggetti designati dalla Capogruppo.

Quesito 3
Il documento in consultazione afferma che all'interno dei gruppi bancari «*l'esternalizzazione delle funzioni aziendali di controllo presso la capogruppo o le altre componenti del gruppo è consentita indipendentemente dalle dimensioni e dalla complessità operativa» a condizione che siano rispettai precisi criteri fra i quali si legge «all'interno di tutte le banche del gruppo e delle altre entità che, a giudizio della capogruppo, assumono rischi considerati rilevanti per il gruppo nel suo complesso vengono individuati appositi referenti i quali: svolgono compiti di supporto per la funzione aziendale di controllo esternalizzata; riportano funzionalmente e gerarchicamente a quest'ultima; provvedono tempestivamente a segnalare eventi o situazioni particolari, suscettibili di modificare i rischi generati dalla controllata*». Nella nota (26) riferita a questo specifico criterio si legge infine «*A seconda della funzione aziendale di controllo esternalizzata può trattarsi di responsabili di unità di controllo del rischio locali, "compliance officer", responsabili di unità distaccate di internal audit*.».

---

modalità e la frequenza della reportistica dovuta al referente per l'attività esternalizzata e agli organi aziendali sulle verifiche effettuate. Resta fermo l'obbligo di dare riscontro tempestivamente a qualsiasi richiesta di informazioni e consulenza da parte di questi ultimi che in ogni caso rimangono responsabili del corretto espletamento delle attività di controllo esternalizzate".

Con riferimento a quanto sopra, e con specifico riferimento alla funzione di compliance, ci chiediamo se, in questo contesto, è corretto far coincidere la nozione di *compliance officer* con quella di responsabile della funzione di *compliance* e pertanto se la banca che esternalizza la funzione deve comunque attribuire al referente il suddetto ruolo oppure se il responsabile della funzione di *compliance* della controllata possa essere chi ricopre questa carica nell'*outsourcer*?
Qualora il referente interno non abbia il ruolo di responsabile della funzione di compliance ci chiediamo inoltre se costui sia responsabile nei confronti dei propri organi aziendali e delle Autorità di vigilanza di eventuali carenze nell'attività di compliance svolta dall'*outsourcer*.

Quesito 4
Per quanto concerne il sistema dei controlli interni nei gruppi bancari il documento in parola prevede che "*Per verificare la rispondenza dei comportamenti delle società appartenenti al gruppo agli indirizzi della capogruppo, nonché l'efficacia del sistema dei controlli interni, la capogruppo si attiva affinché, nei limiti dell'ordinamento,* ***la funzione di revisione interna*** *a livello consolidato effettui periodicamente verifiche in loco sulle componenti del gruppo, tenuto conto della rilevanza delle diverse tipologie di rischio assunte dalle diverse entità.* ***La capogruppo*** *invia annualmente alla Banca d'Italia* ***una relazione riguardante gli accertamenti effettuati sulle società controllate****, contenente anche le considerazioni dei propri organi aziendali*".

La formulazione dell'ultimo paragrafo citato, in particolare se letto separatamente dal paragrafo che lo precede, induce dei dubbi in merito agli accertamenti oggetto di relazione annuale. In particolare si ritiene opportuno chiarire se si faccia riferimento alle sole verifiche della funzione di revisione interna (presupponendo un collegamento con quanto previsto nel paragrafo precedente quello in esame) oppure a tutti gli accertamenti condotti - anche dalle altre funzioni di controllo - relativi alle varie componenti del gruppo.

SEZIONE VI

IMPRESE DI RIFERIMENTO

SEZIONE VII

PROCEDURE DI ALLERTA INTERNA

Con riferimento alle procedure di allerta interna, oltre a richiedere che essa sia adeguatamente calibrata secondo il principio di proporzionalità, ci si chiede se possa essere ipotizzato un meccanismo telematico di comunicazione (che tuteli la privacy del segnalante e dell'eventuale segnalato) che possa riferire ad un'unica funzione (da far coincidere con una funzione di controllo, in quanto già abituata ad operare su dati e notizie riservate e confidenziali), incaricata poi di interessare, di volta in volta, la struttura che dovrà attivarsi.

Nell'indagine sullo stato dell'arte e le prospettive della funzione di compliance nelle banche italiane condotta dall'ABI nel 2011 già citata alla nota 6 è emerso che, anche in relazione all'importanza del rischio di conformità nel settore bancario (componente legale e reputazionale) la maggioranza dei 40 rispondenti ritiene utile l'implementazione di una policy Aziendale di *Whistle Blowing* ma solo con molteplici cautele dato il contesto culturale di riferimento. Più nel dettaglio rispetto ad eventuali sistemi di *Whistle Blowing* quello da preferire dovrebbe prevedere: segnalazioni potenzialmente effettuabili da tutti i dipendenti, solo su determinati temi, solo in forma scritta, corredate dove possibile da documentazioni.

In argomento, occorre segnalare che il Garante per la protezione dei dati personali – a seguito di istanza di verifica preliminare formulata da una associata ABI e veicolata all'Autorità con lettera ABI del 30 gennaio 2009 e di altre richieste di analogo tenore – ha emanato, in data 10 dicembre 2009, un Provvedimento con cui ha segnalato al Parlamento e al Governo *"l'opportunità che sia valutata, in relazione all'utilizzo di sistemi di segnalazione di presunti illeciti commessi da soggetti operanti a vario titolo nell'ambito di un'organizzazione aziendale, l'adozione di apposite disposizioni legislative*", volte a chiarire la portata e i limiti di tale sistema.

SEZIONE VIII

SUCCURSALI DI BANCHE COMUNITARIE E DI BANCHE EXTRACOMUNITARIE AVENTI SEDE NEI PAESI DEL GRUPPO DEI DIECI O IN QUELLI INCLUSI IN UN ELENCO PUBBLICATO DALLA BANCA D'ITALIA

SEZIONE IX

INFORMATIVA ALLA BANCA D'ITALIA

A)

Sarebbe opportuno prevedere alla sezione IX (Informativa alla Banca d'Italia), relativamente alla trasmissione tempestiva alla Banca d'Italia delle relazioni sull'attività svolta redatte periodicamente dalle funzioni di controllo, anche le relazioni della funzione antiriciclaggio.

* * *

Quesito
Il documento prevede che "Le banche trasmettono alla Banca d'Italia tempestivamente, le relazioni sull'attività svolta redatte annualmente dalle funzioni di controllo dei rischi, di conformità alle norme e di revisione interna. **Se una o più di queste funzioni sono esternalizzate, la relazione è redatta dal referente aziendale**".

Si chiede in particolare di chiarire la competenza e la responsabilità della redazione della relazione di cui trattasi nel caso in cui la Società controllata abbia esternalizzato una o più funzioni di controllo alla capogruppo provvedendo alla nomina da parte del Consiglio di Amministrazione del responsabile della funzione stessa quale responsabile della funzione di controllo della Società controllata. Nel caso in parola, attenendosi alla formulazione presente nel documento per la consultazione, parrebbe che la relazione debba essere redatta da un referente della Società controllata che non coinciderebbe, date le premesse, con il responsabile aziendale della funzione di controllo. Qualora fosse confermata tale impostazione si chiede cortesemente di chiarire il ruolo, le responsabilità e le competenze del citato "referente aziendale".

SEZIONE X

DISPOSIZIONI ABROGATE

ALLEGATO A

DISPOSIZIONI SPECIALI RELATIVE A PARTICOLARI CATEGORIE DI RISCHIO

1. Premessa

2. Rischio di credito e di controparte

2.1 Valutazione del merito di credito

Nell'allegato A- Disposizioni speciali relative a particolari categorie di rischio viene menzionata l'importanza per i rischi di credito della disponibilità di base dati complete ed aggiornate, di un sistema informativo che ne consenta lo sfruttamento ai fini richiesti, di un'anagrafe clienti attraverso cui generare ed aggiornare…..i dati identificativi della clientela, le connessioni giuridiche ed economico-finanziarie tra clienti diversi….. lasciando intravedere margini di libertà alle Banche in tema di ripartizione dei controlli di primo e di secondo livello per tale ambito, nel rispetto dei principi di carattere generale indicati nel Capitolo 7-Sezione I. Si ritiene opportuno precisare anche entro quali limiti (es. in caso di assenza di poteri deliberativi significativi) e/o con quali modalità (es. definizione di dettaglio del perimetro di responsabilità e delle modalità di interrelazione con le funzioni di controllo) possano se del caso essere effettuati **controlli di primo livello seconda istanza e/o di secondo livello anche da parte di strutture organizzative solitamente non esercitanti le funzioni di controllo richiamate nel documento** (es. controlli sulla filiera del credito effettuati da strutture creditizie).

In merito al tema della valutazione del merito di credito (TIT. V, Cap. 7, All. A, Par. 2.1): la nuova normativa in consultazione richiede che le banche:

- si dotino "*di metodologie interne che consentano una valutazione del rischio di credito derivante da esposizioni nei confronti di singoli prenditori, titoli, posizioni verso le cartolarizzazioni nonché del rischio di credito a livello di portafoglio. Tali metodologie non devono basarsi meccanicamente sulle valutazioni espresse dalle ECAI*";
- effettuino "*con periodicità almeno annuale, una specifica valutazione della complessiva coerenza dei rating delle ECAI con le valutazioni elaborate in autonomia*".

Seppure questo tema sia già stato oggetto di una specifica comunicazione dal parte della Banca d'Italia, si ritiene opportuno che nella versione finale del documento in consultazione si articoli meglio la previsione per portafogli e/o secondo il criterio di proporzionalità.
Ad esempio, **si richiede che il requisito normativo in esame possa intendersi limitato alle controparti corporate e bancarie**, non considerando necessaria, o eventualmente solo per le banche di maggiori dimensioni in applicazione del principio di proporzionalità, una valutazione anche del merito di credito delle controparti sovrane, per le quali tale valutazione sarebbe ulteriormente complessa.

3. Rischi derivanti dall'utilizzo di tecniche di attenuazione del rischio di credito

4. Concentrazione dei rischi

Si chiede di eliminare nel testo la parte "incluse le controparti centrali" .

Infatti, considerando tra queste anche i soggetti vigilati a livello Europeo, tra cui la BCE e le altre clearing houses che rendono più trasparente e regolamentato il mercato, l'introduzione di un riferimento ad un connesso rischio di concentrazione non appare necessario e condivisibile, quanto più considerando che il complesso della regolamentazione in divenire stia spingendo verso un accentramento di molte transazioni (esempio i derivati) vs le controparti centrali private e la necessità di limitare i rischi di wrong way abbia accentuato la necessità di ricorrere a soggetti pubblici e privati vigilati per rendere più robusto il sistema finanziario.

5. Rischi derivanti da operazioni di cartolarizzazione

6. Rischi di mercato

7. Rischio tasso di interesse derivante da attività non appartenenti al portafoglio di negoziazione a fini di vigilanza

8. Rischi operativi

9. Rischio di liquidità

10. Rischio di leva finanziaria eccessiva

Si chiede di non introdurre tale previsione che, anche nel contesto del *level playing field* internazionale rappresenterebbe una anticipazione di notevole portata, ed in ogni caso riferita solamente ad una tipologia di leva non necessariamente coordinata con l'impianto normativo del *leverage ratio*. In particolare, fintanto che non sia chiarito il quadro

internazionale dei principi contabili e della loro applicazione a livello di Vigilanza Prudenziale, la norma potrebbe distorcere una corretta gestione complessiva del rischio da parte degli intermediari. In ogni caso, data la situazione attuale ed il quadro di indeterminatezza normativa, si dovrebbe quantomeno valutare il rischio quale potenziale impatto sul patrimonio di vigilanza, piuttosto che sul patrimonio contabile.

11. Rischi connessi con l'emissione di obbligazioni bancarie garantite

12. Rischi connessi con l'assunzione di partecipazioni

13. Attività di rischio e conflitti di interesse nei confronti di soggetti collegati

14. Rischi connessi con l'attività di banca depositaria di OICR e fondi pensione

ALLEGATO B CONTROLLI SULLE SUCCURSALI ESTERE

Si sollecita la indicazione a titolo esemplificativo dei criteri qualitativi e quantitativi sulla base dei quali individuare l'"operatività significativa".
Al riguardo si ritiene possano rilevare : aspetti inerenti le autonomie deliberative, la tipologia dei prodotti commercializzati, la legislazione locale di riferimento.

TITOLO V - CAPITOLO 8 SISTEMA INFORMATIVO

SEZIONE I DISPOSIZIONI DI CARATTERE GENERALE

1. Premessa

2. Fonti normative

3. Destinatari della disciplina

4. Definizioni

A)

Sulla base di quanto descritto all'interno del Box 4, si propone di modificare la definizione di "utente responsabile" come segue:

"utente ***dell'applicazione*** ~~*responsabile (system owner)*~~*", la figura aziendale identificata o identificabile* ~~*per ciascun sistema*~~ *che* ***svolge il ruolo di referente interno dell'applicazione e si rapporta*** ~~*ne assume la generale responsabilità amministrativa*~~ ~~*in rappresentanza degli utenti,*~~ ~~*in rapporto*~~ *con le funzioni preposte allo sviluppo e alla gestione tecnica* ***in qualità di rappresentante degli utenti che fruiscono di tale applicazione (es. funzioni di business);***

B)

Con riferimento alla definizione di "operazioni critiche", si evidenzia la necessità di rivedere tale definizione allo scopo di ancorare le disposizioni previste per l'attività di tracciamento delle operazioni svolte alle previsioni già esistenti in tema di trattamento dei dati personali e in ogni caso di consentire una segmentazione delle tipologie di dati da registrare sulla base della rilevanza di business e del livello di rischio associato. Si fa riferimento in particolare all'ultimo alinea del punto elenco al par.2 della sezione IV.

SEZIONE II GOVERNO E ORGANIZZAZIONE DELL'ICT

Numerose banche, in particolare le realtà di minore dimensione e complessità operativa, hanno da tempo affidato in outsourcing l'intero sistema informativo, con l'obiettivo di accrescere l'efficienza e condividere gli investimenti necessari all'adeguamento del sistema informativo sia ai cambiamenti tecnologici e di mercato che alle significative e numerose variazioni del contesto normativo.
Al fine di applicare il principio di proporzionalità alle norme inserite nella presente sezione, si ritiene opportuno segnalare che l'interazione tra la banca e l'outsourcer – sia in relazione ai compiti degli organi aziendali, sia più in dettaglio in merito all'architettura dei sistemi informativi, alle policy di sicurezza, alle metodologie per l'analisi del rischio informatico – può sottendere differenti modalità di generazione dei documenti sottoposti all'approvazione degli organi aziendali.

1. Compiti dell'organo con funzione di supervisione strategica

Allo scopo di evitare un'interpretazione del termine "valore" eccessivamente quantitativa, si propone di modificare il quarto alinea del primo elenco puntato come segue:

- *è informato con cadenza almeno annuale* ***sullo stato dei*** ~~*sul valore fornito all'azienda dai*~~ *sistemi informativi, in termini di adeguatezza dei servizi erogati e del supporto prestato all'evoluzione del business, in rapporto ai costi sostenuti; è inoltre informato tempestivamente in caso di gravi problemi per l'attività aziendale derivanti da incidenti e malfunzionamenti rilevanti del sistema informativo.*

2. Compiti dell'organo con funzione di gestione

I compiti dell'organo con funzioni di gestione sembrano in alcuni casi essere caratterizzati da un eccessivo livello di dettaglio o far riferimento ad attività già adeguatamente presidiate da altre funzioni di controllo (es. Internal Audit).

Si propone pertanto di modificare il secondo alinea del primo elenco puntato come segue:

- ***approva*** ~~*disegna e segue l'implementazione dei*~~ *i processi di gestione dell'ICT – incluso in particolare il processo di analisi del rischio informatico –* ***e ne monitora l'implementazione****, garantendo l'efficacia ed efficienza dell'impianto nonché la sua completezza e coerenza complessiva, con particolare riguardo ad una chiara e funzionale assegnazione di compiti e responsabilità, alla validità del supporto metodologico e procedurale;*

Si evidenzia la necessità di una modulazione di alcuni compiti dell'organo di gestione nei casi di full outsourcing quali ad esempio:
a) la definizione della struttura organizzativa della funzione ICT con specifico riferimento anche al "corretto dimensionamento quali-quantitativo delle risorse umane assegnate";
b) l'assegnazione di compiti e responsabilità all'interno della funzione ICT.
A tal proposito si chiede in particolare di chiarire la compatibilità di tali previsioni con una situazione di full outsourcing laddove non è pregiudicata certamente la possibilità di indirizzo, monitoraggio e controllo dei servizi prestati ma possono esistere difficoltà nell'influenzare tali aspetti autonomamente gestiti dall'Outsourcer.

3. Organizzazione della funzione ICT

A)

Allo scopo di abilitare le autonome scelte organizzative degli intermediari, si ritiene di poter interpretare lo spirito della norma ipotizzando che il neo istituito Direttore dei Sistemi Informativi possa non dover riportare gerarchicamente all'organo con funzione di gestione ma sia sufficiente prevedere adeguati legami funzionali e flussi informativi che consentano una più dettagliata informativa a questo organo in materia ICT. Nella situazione attuale, infatti, presso molte banche il CIO riporta o al Direttore Generale/Amministratore Delegato o al COO (Chief Operating Officer), i quali, pur essendo talvolta parte del Board of Executive, non sempre appartengono all'organo con funzione di gestione.

Si propone pertanto la seguente modifica al primo alinea:

- *la previsione, nelle realtà più complesse, di un organo ("Direttore dei sistemi informativi" o equivalente) che assume la generale responsabilità della funzione,* ***che predisponga periodicamente flussi informativi strutturati*** ~~*con linea di riporto diretta*~~ *verso l'organo con funzione di gestione ([4]), a garanzia dell'unitarietà della visione gestionale e* ***dell'implementazione delle azioni di mitigazione*** *del rischio informatico nonché dell'uniformità di applicazione delle norme riguardanti i sistemi informativi;*

B)

Si evidenzia come le previsioni dell'intero paragrafo, nonostante vengano mitigate in due punti dalla dicitura "nelle realtà più complesse", di fatto risultano, in termini di rapporto costi/benefici, eccessivamente onerose per le banche di minore dimensione e complessità operativa.
Si propone dunque di modificare il terzo alinea come segue:

- *la realizzazione degli opportuni meccanismi di raccordo con le linee di business, con particolare riguardo alle attività propedeutiche all'individuazione e pianificazione delle iniziative informatiche (****nelle realtà più complesse può richiedere la definizione di un processo di*** *raccolta della domanda di servizi*

informatici e promozione delle opportunità tecnologiche offerte dall'evoluzione dei sistemi ICT);

C)

Inoltre, si evidenzia che realtà complesse, con una funzione ICT più articolata, necessitano di chiarire la possibile separazione delle funzioni previste nel secondo alinea, che si propone di modificare come segue:

- *la chiara attribuzione di responsabilità per la pianificazione e il controllo unitario del portafoglio dei progetti informatici**; ove la complessità operativa lo renda necessario, l'attribuzione di responsabilità per il governo dell'evoluzione dell'architettura e, non necessariamente congiunta, dell'innovazione tecnologica;***

Nota: nel caso delle realtà in full outsourcing, tale compito si ritiene possa essere svolto nell'ambito dei comitati utente appositamente costituiti

D)

In aggiunta, si ritiene opportuno fare univocamente riferimento alla funzione di sicurezza informatica, senza richiamare il concetto di sicurezza delle informazioni, non necessariamente coincidente. Più in particolare, con riferimento all'analisi del rischio informatico e di emanazione e verifica della policy di sicurezza ICT, si rimanda a quanto espresso nel Box 4.

SEZIONE III LA GESTIONE DEL RISCHIO INFORMATICO

A)

Come già evidenziato all'interno del Box 4, la norma sembra avallare l'interpretazione secondo cui la figura denominata come "utente responsabile" è l'unico responsabile del processo di valutazione dei rischi, nonostante le specifiche competenze tecniche che tale processo richiede.
Si propone pertanto la seguente modifica:

*Il processo di analisi deve essere svolto ~~dall'utente responsabile ([5]) con la partecipazione del personale tecnico~~ **dalle funzioni specialistiche con la partecipazione attiva dell'utente dell'applicazione** ([5]), secondo una metodologia definita dall'organo con funzione di gestione. Esso si compone di due fasi successive:*
[…]
*il trattamento del rischio, volto all'individuazione delle misure di sicurezza – di tipo tecnico e organizzativo - idonee a conseguire il contenimento del rischio individuato; le modalità di svolgimento possono variare in dipendenza delle risultanze della fase precedente, ma in ogni caso deve essere determinato il rischio residuo da sottoporre ad accettazione formale dell'utente **dell'applicazione** ~~responsabile~~ ([8]). In tale ambito l'utente **dell'applicazione** ~~responsabile~~, che sarà in generale vincolato all'osservanza del livello di tolleranza al*

rischio definito a livello aziendale, potrà eventualmente considerare l'adozione di misure alternative o ulteriori di trattamento del rischio ([9]).

B)

Inoltre, appare opportuno dettagliare maggiormente il concetto di "gestione del rischio informatico" allo scopo di dare evidenza alla funzione di sicurezza informatica in quanto preposta tra l'altro alla definizione (ma non all'implementazione, generalmente in capo alla funzione IT) delle contromisure volte alla mitigazione del rischio e, conseguentemente, alla riduzione del rischio residuo. Si propone dunque di modificare il primo paragrafo come segue:

*Il processo di analisi **e mitigazione** del rischio informatico costituisce un importante strumento aziendale a garanzia dell'efficacia ed efficienza dei sistemi di protezione, permettendo **alla funzione di sicurezza informatica (Sezione IV)** di graduare le misure di sicurezza in funzione degli specifici rischi ravvisati nei diversi ambienti; ~~inoltre esso riveste un fondamentale ruolo di raccordo tra i processi di governo dei sistemi informativi (Sezione II) e le attività tecnico – gestionali della sicurezza informatica (Sezione IV).~~*

C)

Riguardo alle metodologie di gestione del rischio informatico, si ritiene che le particolari caratteristiche di questo specifico rischio operativo possano abilitare la gestione di un impianto metodologico basato anche su valutazioni di carattere qualitativo. A tal fine, si propone di modificare i due alinea del punto elenco come segue:

*- la valutazione **anche qualitativa** del rischio potenziale […];*
*- […] ma in ogni caso deve essere **valutato** ~~determinato~~ il **livello di** rischio residuo da sottoporre […]*

D)

Nel caso delle realtà in full outsourcing, la gestione del rischio informatico si ritiene possa essere svolta sulla base di analisi tecniche condotte nell'ambito di comitati utente allo scopo costituiti presso l'outsourcer.

E)

Con riferimento ai presidi in aggiunta a quelli già operativi, per i sistemi già in esercizio, la preesistenza della situazione di rischio induce a suggerire un approccio più flessibile in ordine all'attuazione di misure compensative.

Si suggerisce pertanto la seguente modifica:
Per i sistemi già in esercizio, gli eventuali presidi ~~in aggiunta~~ **che la banca decida di aggiungere** *a quelli già operativi, **questi** devono formare oggetto di uno specifico piano di implementazione, con l'indicazione dei tempi di realizzazione. Nelle more dell'attuazione del piano, il rischio residuo **può** ~~deve~~ essere trattato con presidi compensativi, ad esempio*

di tipo organizzativo o procedurale, anch'essi documentati e sottoposti all'accettazione formale dell'utente ***dell'applicazione*** ~~*responsabile*~~*.*

SEZIONE IV IL SISTEMA DI GESTIONE DELLA SICUREZZA INFORMATICA

In linea con il titolo della presente Sezione, si propone di modificare il primo capoverso come segue:
"Il sistema di gestione della sicurezza informatica ha l'obiettivo di garantire…"

1. Policy di sicurezza

Dai commenti ricevuti emerge come nel testo non vi sia un pieno allineamento rispetto alla terminologia utilizzata: si evidenzia, in particolare, che la Sezione IV è focalizzata sulla gestione della sicurezza informatica mentre, nel primo alinea del punto elenco, si fa riferimento al "sistema di gestione della sicurezza delle informazioni" che comprende diversi ambiti oltre alla sola componente informatica.
Si suggerisce, pertanto, un allineamento della terminologia, in linea con quanto disposto nel presente capitolo.

In particolare, si propone di denominare il paragrafo in oggetto come "Policy di sicurezza **informatica**" e di modificare il primo capoverso come segue:

"La policy di sicurezza informatica, ***predisposta dalla funzione con competenza specialistica,*** *deve essere approvata dall'organo con funzione di supervisione strategica e comunicata a tutto il personale nonché alle terze parti esterne coinvolte nella gestione di informazioni e sistemi".*

2. La sicurezza dei dati e il controllo degli accessi

L'ultimo alinea del punto elenco fa riferimento alla registrazione e conservazione delle tracce elettroniche e sembra pertanto essere fortemente in relazione con quanto già disposto dall'Autorità Garante per la Protezione dei Dati Personali nel Provvedimento del 12 maggio 2011 in materia di circolazione delle informazioni bancarie e tracciamento delle operazioni bancarie, richiamato in nota 16. Si ritiene opportuno chiarire che le tipologie di operazioni oggetto di tracciamento sono da considerarsi coincidenti tra i due provvedimenti, allo scopo di perseguire l'obiettivo di armonizzazione del quadro normativo esistente.
Rileva evidenziare come il Provvedimento in oggetto disponga che la conservazione dei file di log sia di 24 mesi per le informazioni riferite alle operazioni bancarie effettuate sui dati bancari. Si ritiene pertanto opportuno allineare i tempi di conservazione riportandoli a 24 mesi, i contenuti dei log e il perimetro di dati e operazioni oggetto di tracciamento, riformulando opportunamente la definizione di operazione critica e modificando l'alinea come segue:
[…] Il periodo di conservazione per le tracce elettroniche in discorso non deve essere inferiore a ***due*** ~~*cinque*~~ *anni ([16]).*

A ulteriore rafforzamento di tale proposta, si evidenzia che il prolungamento di tre anni dei tempi di conservazione delle operazioni, anche solo di consultazione, comporterebbe un ulteriore, significativo incremento di costi a carico del sistema.

3. La gestione dei cambiamenti

4. La gestione degli incidenti di sicurezza

Si ritiene utile inserire un esplicito riferimento agli Event Type del rischio operativo, al fine di avere un linguaggio comune e per effettuare eventuali analisi di confronto settoriale. In particolare, si propone di inserire la seguente frase al termine del primo capoverso:

Le frodi informatiche e gli attacchi attraverso internet possono essere classificati come: Event Type 01.02 se riconducibili a frode da personale interno alla banca, Event Type 02.02 se riconducibili a frode da soggetti esterni alla banca. Gli eventi causati da gravi malfunzionamenti e disservizi possono essere classificati come Event Type 06.01 "Perdite dovute a disfunzioni/indisponibilità dei sistemi informativi".

5. La disponibilità delle informazioni e dei servizi ICT

SEZIONE V IL SISTEMA DI GESTIONE DEI DATI

In merito alla definizione di un sistema di gestione dei dati, occorre evidenziare che un approccio che non contemperi le differenze esistenti tra le tipologie e la criticità di dati gestite dalla banca rischia di rivelarsi eccessivamente oneroso da un punto di vista economico e gestionale. Per cogliere questo spunto e abilitare logiche di prioritizzazione degli interventi si suggeriscono le seguenti modifiche al secondo alinea del punto elenco:

- *è definito uno standard aziendale di data governance, che individua ruoli e responsabilità* ***di tutte le*** ~~*delle*~~ *funzioni coinvolte* ***nell'utilizzo e*** *nel trattamento dell'informazione,* ***non solamente IT****, nonché le misure atte a garantire la qualità dei dati (in termini di completezza e accuratezza) ([24]),* ***anche segmentando le tipologie del dato e i processi,*** *sia operativi che gestionali ([25]),* ***in termini di rilevanza e tempi di implementazione****;*

SEZIONE VI L'ESTERNALIZZAZIONE DI SISTEMI E SERVIZI ICT

1. Tipologie di esternalizzazione

A)

A commento di quanto disposto nel terzo capoverso del presente paragrafo, con particolare riferimento alla previsione di opportune *exit strategies*, si evidenzia come tale possibilità sia difficoltosa da realizzare da parte delle realtà di minore dimensione e complessità operativa, che da tempo hanno affidato in outsourcing l'intero sistema informativo.

B)

Inoltre, appare opportuno specificare che, nel caso di affidamento di sistemi e servizi ICT a società strumentali di gruppo, è necessario che non siano applicate le disposizioni in particolare legate al contenimento del grado di dipendenza dal soggetto cui sono affidati i sistemi (in virtù della sua appartenenza al gruppo bancario), il mantenimento presso le singole banche delle competenze e la previsione di *exit strategies*.

2. Accordi con i fornitori e altri requisiti

A)

Con riferimento alla esternalizzazione di sistemi e servizi ICT presso fornitori che utilizzano data center in paesi diversi dall'Italia, si ritiene opportuno escludere dall'obbligo di comunicazione preventiva le situazioni in cui il servizio di Disaster Recovery offerto abbia un ulteriore back up in paesi UE. In tale situazione, infatti, la localizzazione all'estero di dati della banca avverrebbe solo nel caso in cui, a seguito di disastro presso la banca, il servizio di Disaster Recovery in Italia fosse a sua volta indisponibile e, in ogni caso, avrebbe carattere temporaneo ed emergenziale. Si propone, a tal proposito, l'inserimento della seguente nota dopo le parole "da quest'ultimo":

Nota: Tale previsione non si applica nel caso di servizi di Disaster Recovery offerti in Italia con ulteriore back up in paesi diversi.

B)

Nel terzo alinea del punto elenco si dispone che vengano periodicamente messe a disposizione dell'intermediario delle copie di back up dei dati. Appare opportuno chiarire che, in particolare per quelle realtà che hanno affidato in full outsourcing il proprio sistema informativo, tale previsione possa essere attuata presso il sito secondario in ottica di Disaster Recovery.

C)

Rispetto all'esternalizzazione di sistemi e servizi ICT, si chiede se occorra segnalare all'Autorità di Vigilanza informazioni anche sui contratti già in essere.

3. Indicazioni particolari

ALLEGATO A DOCUMENTI AZIENDALI PER LA GESTIONE E IL CONTROLLO DELL'ICT

ALLEGATO B MISURE IN MATERIA DI SERVIZI TELEMATICI PER LA CLIENTELA

1. Verifica dell'autenticità del sito web e cifratura del canale di comunicazione

2. Procedura di autenticazione del cliente

3. Autorizzazione e monitoraggio delle transazioni di pagamento

4. Sensibilizzazione della clientela

TITOLO V – CAPITOLO 9 DISPOSIZIONI IN MATERIA DI CONTINUITÀ OPERATIVA

Con riferimento all'ipotesi di enucleare il presente capitolo dal documento complessivo, si evidenzia che l'integrazione di tale tematica rispetto al sistema dei controlli interni e, più in generale, alla capacità della banca di essere resiliente di fronte a problematiche di vario genere, rappresenta uno sforzo positivo di razionalizzazione del corpo normativo. D'altra parte, si comprende e si condivide l'esigenza di indirizzare efficacemente le misure indirizzate ai soggetti non bancari previste da questo capitolo.
Pertanto, si propone, con riferimento alle banche, di mantenere il testo nell'ambito delle Istruzioni di Vigilanza e, con riferimento agli altri soggetti, di enucleare un testo identico che contenga anche i riferimenti alla continuità operativa inseriti nel capitolo 7 con riferimento all'Internal Audit e all'esternalizzazione di funzioni aziendali.

1. Destinatari della disciplina

Il testo attuale, contrariamente alla normativa precedente, esplicita i destinatari della disciplina, estendendo il campo di applicazione, oltre alle banche, anche ad altri intermediari. In particolare individua "*i sistemi di pagamento e i relativi fornitori tecnologici*" tra i destinatari delle nuove disposizioni, non fornendo però ulteriori indicazioni sulla definizione di "*sistemi di pagamento*". Si propone di modificare tale locuzione in "infrastrutture qualificate di pagamento", esplicitando pertanto che il perimetro di applicazione della norma comprende i soggetti che svolgono tali attività e non le attività stesse.

2. Premessa

3.Definizioni

Con l'obiettivo di fare chiarezza fra diverse tipologie di tempi citate e definite nella normativa e che hanno caratteristiche intrinseche diverse, si propone di inserire le seguenti definizioni:
Tempo obiettivo di ripristino (RTO – Recovery Time Objective): obiettivo di ripristino in termini di periodo di tempo successivo al verificarsi di un incidente necessario per la ripartenza di un processo a un livello di servizio prestabilito.
Punto obiettivo di ripristino (RPO – Recovery Point Objective): obiettivo di ripristino in termini di perdita di dati ammissibile, ovvero periodo di tempo massimo che intercorre tra l'ultimo salvataggio dei dati e il momento di blocco del processo che li utilizza.
Tempo massimo accettabile di interruzione del servizio: tempo oltre il quale diventa inaccettabile l'impatto negativo derivante da una interruzione di servizio conseguente a una situazione sfavorevole.

4. Ambito del piano di continuità operativa

A)

Con riferimento agli scenari di crisi che devono essere presi in considerazione, si suggeriscono alcune modifiche tese a rappresentare più chiaramente le situazioni di indisponibilità che occorre valutare, nell'ottica di seguire l'approccio per impatti derivanti da mancanza di una risorsa critica che costituisce la cifra della continuità operativa nel settore bancario italiano.
In particolare, viene citata l'eventualità di "alterazione dei dati o indisponibilità dei sistemi a seguito di attacchi perpetrati dall'esterno attraverso reti telematiche", dicitura che rischia di limitare l'indisponibilità dei sistemi ICT al solo evento di attacchi provenienti dall'esterno.
Si suggerisce di separare tale punto in due componenti, l'una focalizzata sulla fattispecie in cui si verifica l'alterazione di dati (integrando tale previsione con la specificazione della semplice indisponibilità dei dati e inserendo inoltre il riferimento ai "documenti critici"), l'altra, riferita ai sistemi informativi, che estende l'indisponibilità alle varie possibili cause.
Si propone pertanto di modificare il quarto alinea del punto elenco come segue:

- alterazione~~ dei dati o indisponibilità dei sistemi a seguito di attacchi perpetrati dall'esterno attraverso reti telematiche~~ **o perdita di** dati **e documenti critici**;
- **indisponibilità dei sistemi informativi critici**;

B)

Tra gli scenari di crisi viene inoltre prevista l'eventualità che si verifichino "danneggiamenti gravi provocati da dipendenti". In ordine a tale scenario, si pongono all'attenzione due riflessioni: l'approccio alla continuità operativa è tipicamente per impatti legati all'indisponibilità di una risorsa critica e lo scenario qui proposto può essere agevolmente ricondotto all'indisponibilità delle risorse danneggiate; da un punto di vista gestionale, la specificità attribuibile ai danneggiamenti provocati dai dipendenti è attentamente analizzata nell'ambito del rischio operativo e della sicurezza informatica. Pertanto, si propone di eliminare tale eventualità tra gli scenari di crisi previsti dalle disposizioni.

C)

Infine, si ritiene possa essere utile al fine di promuovere la contaminazione fra diverse culture presenti in banca, e segnatamente quella della continuità operativa e del risk management, accennare al fatto che gli scenari di crisi, una volta manifestatisi, possono produrre perdite economiche che daranno l'avvio al processo di analisi ex post delle cause per l'associazione agli Event Type che, nel caso specifico, li avranno generati.

5. Correlazione ai rischi

6. Definizione del piano e gestione dell'emergenza

Allo scopo di dare completezza di visione al Capitolo 9 contenente disposizioni in materia di continuità operativa, si suggerisce di ripristinare il paragrafo relativo alle responsabilità degli organi aziendali, per maggior chiarezza richiamate anche nel Capitolo 7, Sezione II.
Si suggerisce pertanto di inserire il seguente paragrafo, con la conseguente traslazione dei paragrafi successivi:

6.1 Ruolo degli organi aziendali
I vertici aziendali promuovono lo sviluppo, l'aggiornamento e le verifiche del piano di continuità operativa, garantendo che il tema della continuità operativa sia adeguatamente considerato a tutti i livelli di responsabilità.
L'organo con funzione di supervisione strategica stabilisce gli obiettivi e le strategie di continuità del servizio; assicura risorse umane, tecnologiche e finanziarie adeguate per il conseguimento degli obiettivi fissati; approva il piano; viene informato, con frequenza almeno annuale, sulla adeguatezza dello stesso.
L'organo con funzione di gestione nomina il responsabile del piano di emergenza; promuove il controllo periodico del piano e l'aggiornamento dello stesso a fronte di rilevanti innovazioni organizzative, tecnologiche e infrastrutturali nonché nel caso di lacune o carenze riscontrate ovvero di nuovi rischi sopravvenuti; approva il piano annuale delle verifiche delle misure di continuità ed esamina i risultati delle prove.
L'attività svolta e le decisioni assunte sono adeguatamente documentate.

6.1 I processi critici

Nell'ambito dell'attribuzione delle responsabilità legate alle misure di continuità dei processi critici, si ritiene opportuno dare maggiore enfasi alla necessità che il responsabile del processo operi in pieno accordo con le misure stabilite nel piano di continuità.
A tal fine si propone la seguente modifica:

Il responsabile del processo, ***in accordo con gli indirizzi strategici e con le regole stabilite nel piano****, individua il tempo massimo accettabile di interruzione del servizio e collabora attivamente alla realizzazione delle misure di continuità ~~in accordo con gli indirizzi strategici e con le regole stabilite nel piano~~.*

6.2 La responsabilità del piano

Allo scopo di assicurare l'omogeneità dei termini utilizzati con riferimento alla continuità operativa, si propone di adottare sempre le diciture "stato di crisi" anziché "stato di emergenza" e "piano di continuità operativa" anziché "piano di emergenza".

6.3 Il contenuto del piano

Per dare maggiore chiarezza alle previsioni in merito alla frequenza dei back-up, anche in ragione dell'elevato impatto economico di un eventuale fraintendimento delle stesse, si propone di modificare il quinto capoverso come segue:
La frequenza dei back-up è correlata al volume di operatività dell'intermediario; gli archivi di produzione ***dei sistemi critici*** *sono duplicati almeno giornalmente. Sono assunte cautele*

per il tempestivo trasporto e la conservazione delle copie elettroniche in siti ad elevata sicurezza fisica posti in luoghi remoti rispetto ai sistemi di produzione.

6.4 Le verifiche

A)

L'estensione raggiunta dai piani di continuità operativa in termini di processi critici rende sempre più articolati i piani dei test messi in atto dalle banche. Nell'esperienza comune a un test tecnico (Disaster Recovery) svolto nelle modalità definite dalla normativa, si affiancano esercitazioni più complessive che, simulando uno o più scenari, testano anche misure organizzative. Per tale ragione, si ritiene opportuno estendere la terminologia adottata in questo paragrafo per riflettere tale approccio, contemperando allo stesso tempo la possibilità di una rotazione dei processi sottoposti a verifica ogni anno.
Si propone pertanto di modificare il paragrafo come segue:

Le verifiche delle misure di ***continuità operativa*** ~~*emergenza*~~ *sono correlate ai rischi e alle criticità dei processi; di conseguenza sono ipotizzabili differenti frequenze e livelli di dettaglio delle prove. In alcuni casi può essere sufficiente la simulazione parziale dell'evento catastrofico; per i processi più critici le verifiche prevedono il coinvolgimento degli utenti finali, degli outsourcer e, qualora possibile, delle controparti rilevanti.*
Con frequenza almeno annuale ***vengono svolte*** ~~*viene svolta una*~~ ***verifiche*** ~~*complessiva*~~*, il più possibile* ***realistiche****, del ripristino della operatività* ***dei processi critici*** ~~*condizioni di emergenza*~~*, effettuando il controllo della funzionalità* ~~*e delle prestazioni*~~ ~~*dei sistemi secondari*~~ *e riscontrando la capacità dell'organizzazione di attuare nei tempi previsti le misure definite nel piano.*

B)

Inoltre, poiché l'esecuzione delle procedure batch durante le verifiche effettuate con dati a perdere non può essere completa in quanto non può comprendere lo scambio di flussi con l'esterno, si propone di modificare il terzo capoverso come segue:

In particolare, le verifiche annuali dei sistemi informativi devono prevedere l'attivazione dei collegamenti di rete presso il sito secondario, ***l'attivazione*** ~~*l'esecuzione*~~ ***di*** ~~*delle*~~ *procedure batch e – per le banche - l'operatività on-line di almeno una succursale.*

6.5 Le risorse umane

Il personale coinvolto nell'esecuzione delle misure di continuità dei processi critici viene chiamato a svolgere attività anche estremamente complesse che pertanto è difficile immaginare possano essere eseguite da personale completamente non esperto. La pratica più diffusa è che tali procedure siano affidate a personale già al corrente della materia (ad esempio perché addetto a tali mansioni in periodi precedenti) e comunque adeguatamente addestrato sulle misure di emergenza, come previsto dal paragrafo stesso. Pertanto si propone di inserire la seguente precisazione al termine del secondo capoverso del paragrafo:

Le procedure di emergenza sono chiare e dettagliate, in modo da poter essere eseguite anche da risorse non ***impegnate nell'ordinario in tali attività*** ~~*esperte*~~*.*

6.6 Infrastrutture e controparti rilevanti

6.7 Controlli

6.8 Comunicazioni alla Banca d'Italia

Il paragrafo prevede che in caso di incidente grave l'intermediario debba informare tempestivamente la Banca d'Italia; tuttavia il testo non integra le successive disposizioni trasmesse dalle filiali della Banca d'Italia alle banche operanti nei rispettivi territori.
Si suggerisce di integrare il paragrafo aggiungendo, al termine del testo, le seguenti integrazioni:

Inoltre, tenuto conto dell'impatto sul sistema bancario di eventi di particolare gravità, anche se non di rilevanza sistemica per il sistema finanziario, gli intermediari contattano il canale di comunicazione istituito dalla Banca d'Italia per la comunicazione di informazioni e per il coordinamento di situazioni di crisi che interessano un singolo intermediario o un'area territoriale.
Il predetto canale potrà essere utilizzato esclusivamente per segnalare situazioni potenzialmente in grado di bloccare o danneggiare in modo grave l'operatività della rete distributiva di un intermediario, o di una sua parte significativa, per almeno quattro ore ovvero di impedire l'ordinata chiusura della giornata operativa.

7. Requisiti particolari

7.1 Processi a rilevanza sistemica

A)

Allo scopo di evidenziare maggiormente la relazione tra gli intermediari chiamati a rispettare i requisiti particolari e i processi a rilevanza sistemica, alcuni dei quali assumono tale rilevanza solo nel quadro di soggetti caratterizzati da volumi rilevanti, si propone di inserire la seguente frase prima della descrizione dei processi:

*Tali processi vengono denominati, ai fini delle presenti disposizioni, "processi a rilevanza sistemica" per la continuità operativa del sistema finanziario italiano****; i servizi sono nominativamente evidenziati agli intermediari per i quali si caratterizzano come processi a rilevanza sistemica****. Si tratta di un complesso strutturato di attività finalizzate all'erogazione dei seguenti servizi:*

B)

Inoltre, si evidenzia che, nell'ambito della descrizione dei servizi, l'erogazione del contante è richiamata in due punti: tra i servizi di pagamento a larga diffusione e con riferimento alle infrastrutture qualificate. Poiché si ritiene che le fondamentali esigenze di liquidità degli operatori economici non siano compromesse dalla indisponibilità dei punti di erogazione di un singolo intermediario, ma dalla indisponibilità dell'intero circuito, si suggerisce di modificare la descrizione dei processi, riguardo al terzo e quarto alinea come segue:

- servizi di pagamento al dettaglio a larga diffusione tra il pubblico. Sono inclusi: bollettini postali, pagamento delle pensioni sociali, ~~erogazione del contante~~;
*- **con riferimento alle infrastrutture qualificate di sistemi di pagamento,** servizi strettamente funzionali al soddisfacimento di fondamentali esigenze di liquidità degli operatori economici, il cui blocco ha rilevanti effetti negativi sull'operatività degli stessi. Sono inclusi: servizi di gestione delle infrastrutture telematiche per l'erogazione del contante tramite terminale ATM (Bancomat) e di supporto ad applicazioni e servizi rientranti nell'ambito della "Convenzione per la partecipazione al Sistema per la trasmissione telematica di dati" (SITRAD).*

7.2 Responsabilità

7.3 Scenari di rischio

7.4 Siti di recovery

7.5 Tempi di ripristino e percentuali di disponibilità

A)

La normativa in questo paragrafo introduce una significativa novità nella modalità di valutazione dei tempi di ripartenza: immaginare che il conteggio del tempo avvenga a seguito di una dichiarazione formale della situazione di crisi rappresenta una discontinuità forte con impatti procedurali, che richiederà alle banche di lavorare sui processi decisionali per potersi adeguare.

Si ritiene inoltre che, in particolare in ragione della rilevanza delle previsioni qui contenuti ai fini della garanzia della continuità dei processi a rilevanza sistemica, allo scopo di stimolare gli intermediari ad assicurare tempi del processo decisionale per quanto possibile contenuti, si propone di inserire la seguente previsione dopo l'elenco puntato:

Il processo di dichiarazione dello stato di crisi è formalizzato e consente di assicurare l'assunzione di decisioni in tempi coerenti con i tempi di ripristino.

Tale frase lascia all'organizzazione di ciascun intermediario la definizione del processo di dichiarazione della crisi, pur richiedendo che tale processo risulti efficiente dal punto di vista dei tempi assicurati, che dovranno essere proporzionati ai tempi di ripristino.

B)

Inoltre, si ritiene utile evidenziare maggiormente il ruolo del coordinamento interbancario posto in essere dalla Banca d'Italia nell'ambito del CODISE allo scopo di evidenziare che tale coordinamento potrà entrare in funzione nel caso in cui si verifichino situazioni di particolare gravità che possono mettere a rischio il rispetto dei tempi di ripristino; l'obiettivo finale è assicurare in ogni caso la più rapida ripartenza dei processi a rilevanza sistemica.
La frase proposta è la seguente:

*Per i processi a rilevanza sistemica~~, di concerto con le Autorità~~, gli intermediari stabiliscono parametri obiettivo relativi alla disponibilità dei servizi**, di concerto con le Autorità; queste avvieranno gli opportuni meccanismi di coordinamento in funzione delle caratteristiche dell'evento.***

7.6 Risorse

7.7 Verifiche

8. Comunicazioni alla Banca d'Italia

Si ritiene che tale paragrafo dovrebbe essere più correttamente numerato 7.8, in quanto riferito ai processi a rilevanza sistemica.

9. Disposizioni abrogate