ASSIREVI
Associazione Italiana Revisori Contabili

Il Presidente

Spettabile
BANCA D'ITALIA
Servizio Normativa e Politiche di Vigilanza
Divisione Normativa Prudenziale
Via Milano, 53
00184 Roma

31 ottobre 2012

Trasmissione tramite e-mail all'indirizzo di posta elettronica certificata: npv@pec.bancaditalia.it

Oggetto: **DOCUMENTO PER LA CONSULTAZIONE - DISPOSIZIONI DI VIGILANZA PRUDENZIALE PER LE BANCHE – SISTEMA DEI CONTROLLI INTERNI, SISTEMA INFORMATIVO E CONTINUITÀ OPERATIVA**

Con riferimento alla consultazione in oggetto, trasmettiamo in allegato alla presente un documento contenente le osservazioni che la scrivente Associazione si pregia di fornire a codesta spettabile Autorità.

Assirevi rimane a disposizione per qualunque chiarimento ritenuto utile od opportuno.

Con osservanza.

Mario Boella

Allegato menzionato

20123 Milano - Via Vincenzo Monti, 16 - Tel. 02.436950 - Fax 02.437326
e-mail: info@assirevi.it - www.assirevi.it

Risposta ASSIREVI alla consultazione della Banca d'Italia relativa alle disposizioni di vigilanza in materia di sistema dei controlli interni e di sistema informativo delle banche e dei gruppi bancari nonché di continuità operativa delle banche e di altri intermediari

Indice

1. Premessa

ASSIREVI esprime apprezzamento per il documento posto in consultazione da codesta Autorità, relativo a "DISPOSIZIONI DI VIGILANZA PRUDENZIALE PER LE BANCHE - SISTEMA DEI CONTROLLI INTERNI, SISTEMA INFORMATIVO E CONTINUITÀ OPERATIVA" del Settembre 2012 (di seguito, il "Documento"), condividendo la necessità di effettuare una revisione organica della disciplina in materia di funzionamento del sistema dei controlli interni in considerazione anche della evoluzione normativa registratasi negli ultimi anni.

Particolare valore viene attribuito da questa Associazione all'obiettivo di "rafforzare" la capacità delle banche di gestire tutti i rischi aziendali, tenuto conto della esperienza della "recente crisi finanziaria".
ASSIREVI ritiene infatti che tale obiettivo, ove opportunamente recepito e concretamente applicato, non possa che contribuire a migliorare l'attività del revisore esterno, data la rilevanza che il sistema dei controlli assume nella operatività della banca.

In tale ottica, ASSIREVI riconosce specifica valenza a taluni interventi proposti da codesta Autorità quali:

- l'obbligo, da parte dell'organo con funzione di supervisione strategica, di definire il livello di rischio tollerato (c.d. "tolleranza al rischio" o "appetito per il rischio");
- l'adozione di un approccio integrato alla gestione dei rischi e il rafforzamento dei poteri della funzione di controllo dei rischi, che tra l'altro è tenuta a fornire pareri preventivi sulla coerenza con la politica aziendale di governo dei rischi delle operazioni di maggiore rilievo;
- l'obbligo da parte degli organi aziendali di definire il processo per l'approvazione di nuovi prodotti e servizi, l'avvio di nuove attività e l'inserimento in nuovi mercati;
- l'obbligo dell'organo con funzioni di supervisione strategica di definire procedure di allerta interna (*internal alert*) volte a permettere la segnalazione da parte dei dipendenti di eventuali disfunzioni dell'assetto organizzativo o del sistema dei controlli interni, nonché di ogni altra irregolarità nella gestione della banca o violazione delle norme disciplinanti l'attività bancaria;
- l'introduzione di una disciplina organica e aggiornata in materia di sistema informativo.

Sulla base degli approfondimenti condotti dalla Commissione Tecnica Servizi Finanziari, attraverso l'apposita costituzione di un gruppo di lavoro, si formulano qui di seguito, in relazione alle nuove disposizioni, alcuni commenti di carattere generale e talune osservazioni specifiche che ripercorrono i box evidenziati alle pagg. vii-viii del Documento di Consultazione.

2. Commenti di carattere generale

Il ruolo della società di revisione

Nell'ambito del Documento il soggetto incaricato della revisione legale dei conti è nominato in una sola occasione, nell'ambito del par. 5 della Sezione II (cfr. pag. 14).
La constatazione non sorprende: il Documento si occupa infatti dei controlli interni alle banche e ai gruppi bancari e si sofferma, ad avviso di questa Associazione correttamente, sulle attività degli organi aziendali, da un lato, e delle funzioni aziendali di controllo, dall'altro lato, effettivi attori del sistema dei controlli interni. La disciplina regolamentare dei controlli interni delle banche non è viceversa la sede opportuna per disciplinare la posizione di un soggetto – quale quello incaricato della revisione legale – che non fa parte di quel "sistema".
Come noto, infatti, la società di revisione legale si colloca in una posizione del tutto esterna rispetto alla società che conferisce l'incarico e non è assimilabile agli organi sociali, né alle funzioni aziendali chiamate a svolgere attività di controllo interno. Del resto, è altrettanto pacifico che il revisore legale non può e non deve essere coinvolto nei processi decisionali della società sottoposta a revisione.
Il soggetto incaricato della revisione legale dei conti, che non è né organo della società, né funzione aziendale, è quindi condivisibilmente escluso dalla relativa disciplina.
Risulta peraltro altrettanto evidente che la comprensione del sistema dei controlli interni dell'azienda riveste un'importanza fondamentale per il revisore legale, dal momento che i rischi che detto sistema mira a monitorare e contenere possono rappresentare anche rischi di significativi errori nel bilancio, oggetto specifico delle verifiche della società di revisione. Il revisore legale è dunque chiamato a conoscere i rischi della società sottoposta a revisione, identificare quelli che possono avere effetti sul bilancio e comprendere quanto posto in essere dagli organi e dalle funzioni aziendali per evitare che tali rischi conducano a conseguenze negative sull'attività di revisione.

Un sistema di controllo interno adeguato comporterà dunque una maggiore affidabilità complessiva delle informazioni fornite dagli organi aziendali e dalle funzioni aziendali di controllo alla società di revisione legale.
In definitiva, se è pacifico che la società di revisione non rientra tra i soggetti del sistema di controllo interno, pare ragionevole ritenere che essa debba comunque essere coinvolta nei flussi informativi generati nell'ambito di detto sistema.
Tale esigenza pare essere stata puntualmente avvertita da codesta Autorità di Vigilanza: in effetti, il passaggio del Documento in cui è menzionato il soggetto incaricato della revisione legale dei conti è proprio nel paragrafo relativo al coordinamento delle funzioni di controllo ("*il corretto funzionamento del sistema dei controlli interni si basa sulla proficua interazione nell'esercizio dei compiti … fra gli organi aziendali, gli eventuali comitati …, i soggetti incaricati della revisione legale dei conti, le funzioni aziendali di controllo…*" (cfr. pagg. 13 -14, all'inizio del par. 5 della Sezione II).

Al riguardo, ASSIREVI condivide pienamente la proposta circa la predisposizione da parte delle banche di un documento che disciplini il coordinamento fra i soggetti coinvolti a vario titolo nel sistema dei controlli interni, ipotesi che anche questa stessa Associazione aveva avanzato nel corso del Tavolo per la Semplificazione dei Controlli promosso da Consob nel corso del 2011.

In questo contesto, ci permettiamo di suggerire, come possibile spunto di riflessione, l'eventualità di porre ancora maggiore attenzione sull'importanza per la società di revisione di disporre di opportune "*modalità di raccordo*", così come individuate nel Documento, con gli organi aziendali e con le funzioni aziendali di controllo.
Al riguardo, si potrebbe per esempio prevedere che le singole banche definiscano tali modalità di raccordo e gli opportuni flussi informativi anche con il soggetto incaricato della revisione legale dei conti, sempre avendo come punto di riferimento il principio di proporzionalità.
Tali aspetti potrebbero trovare spazio nel documento che dovrebbe essere approvato dall'organo con funzione di supervisione strategica e nel quale, allo stato, dovrebbero essere "*definiti i compiti e le responsabilità dei vari organi e funzioni (aziendali e societarie) di controllo, i flussi informativi tra le diverse funzioni/organi e tra queste/i e gli organi aziendali e, nel caso in cui gli ambiti di controllo presentino aree di potenziale sovrapposizione o permettano di sviluppare sinergie, le modalità di coordinamento e di collaborazione*" (cfr. par. 5, pag. 14, penultimo capoverso).
Nella predisposizione di tale documento, per la parte relativa al flusso informativo nei confronti del soggetto incaricato della revisione, occorrerebbe fare riferimento ai principi di revisione applicabili, in particolare l'ISA 260 (Comunicazione con i responsabili delle attività di governance) e l'ISA 265 (Comunicazione delle carenze nel controllo interno ai responsabili delle attività di governance ed alla direzione), che trattano specificamente la materia in oggetto. In particolare, tra le informazioni oggetto del suddetto flusso informativo, potrebbe essere opportuno prevedere la specifica comunicazione circa la valutazione del rischio effettuata da parte dell'organo di gestione in ordine al fatto che l'attendibilità del bilancio possa essere significativamente compromessa.

La bipartizione "Organi aziendali" e "Funzioni aziendali di controllo"

Il Documento ha, tra gli altri, il pregio di definire e, per così dire, inquadrare chiaramente i protagonisti del sistema dei controlli interni. Tale obiettivo è perseguito attraverso la chiara bipartizione tra:

- gli "*organi aziendali*", che ricomprendono l'"*organo con funzione di supervisione strategica*", l'"*organo con funzione di gestione*" e l'"*organo con funzione di controllo*"; e
- le "*funzioni aziendali di controllo*", che a loro volta includono le funzioni di *compliance*, *risk management* e *internal audit*.

Nel titolo del par. 5 della Sezione II si fa invece riferimento al coordinamento delle "*funzioni di controllo (interne e societarie)*".
La locuzione pare riferirsi a soggetti ulteriori rispetto agli "*organi aziendali*" e alle "*funzioni aziendali*" di controllo, e in particolare:

- da un lato, all'organismo di vigilanza ai sensi del D.Lgs. 231/2001 e al dirigente preposto ex art. 154-bis D.Lgs. 58/1998 ("TUIF") per le banche quotate, che costituirebbero le "*funzioni societarie di controllo*" (citate anche alla Sezione II, par. 2, lett. a) dell'alinea "*approva*", pag. 9); nonché,
- dall'altro lato, ai comitati interni all'organo amministrativo previsti dal Codice di Autodisciplina (che costituirebbero le funzioni "*interne*").

Al riguardo, le funzioni così individuate appaiono di natura eterogenea e non necessariamente coinvolte in attività di controllo.
In particolare, il dirigente preposto risulta avere la responsabilità, tipicamente gestoria, di predisporre adeguate procedure amministrative e contabili per la formazione dei bilanci e la predisposizione delle comunicazioni di carattere finanziario.

Sotto un diverso profilo, i comitati costituiti all'interno dell'organo amministrativo, secondo la più recente versione del Codice di Autodisciplina, avrebbero funzioni sostanzialmente di assistenza, anche istruttoria, e di supporto al *plenum* dell'organo gestorio.

In un'ottica di ancora maggiore chiarezza, si potrebbe dunque valutare di eliminare i riferimenti rinvenibili nel Documento alle funzioni di controllo "*societarie*" e "*interne*", che non paiono agevolmente differenziabili rispetto alla definizione di funzioni di controllo "*aziendali*" e potrebbero dunque creare difficoltà interpretative (favorite, tra l'altro, anche dall'assenza delle relative definizioni nel par. 3 della Sezione I, a ciò dedicato).

La definizione del processo di approvazione di nuovi prodotti da parte dell'organo con funzione di gestione

Il Documento stabilisce "*l'obbligo da parte degli organi aziendali di definire il processo per l'approvazione di nuovi prodotti e servizi, l'avvio di nuove attività e l'inserimento in nuovi mercati (cfr. Capitolo 7, Sezione II, parr. 2 e 3)*". Al riguardo Assirevi ritiene opportuno che nell'ambito di tale processo, da definirsi, secondo quanto indicato nel Documento, dall'Organo con funzione di gestione, sia espressamente prevista la valutazione dell'impatto di nuovi prodotti e servizi sulle procedure amministrative e contabili per la formazione del bilancio di esercizio e, ove previsto, del bilancio consolidato nonché di ogni altra comunicazione di carattere finanziario.

Di conseguenza, Assirevi riterrebbe utile inserire nel Titolo V - Capitolo 7 "*Il sistema dei controlli interni*", Sezione II "*Il ruolo degli organi aziendali*", paragrafo 3 – "*Organo con funzione di gestione*", una nuova lettera nel punto elenco di pagina 12 con il fine di inserire l'obbligo in capo all'organo con funzione di gestione di valutare l'impatto sulle procedure amministrative e contabili per la formazione del bilancio di esercizio e, ove previsto, del bilancio consolidato nonché di ogni altra comunicazione di carattere finanziario.

Organo di controllo e Organismo di Vigilanza

Si ritiene condivisibile che le funzioni di vigilanza ai sensi del D. Lgs. 231/01 siano attribuite all'organo di controllo nell'ottica di evitare rischi di sovrapposizione di compiti e di responsabilità. Peraltro, il trasferimento dei compiti dell'Organismo di Vigilanza ad un organo con funzione di controllo disciplinato da norme di natura prescrittiva potrebbe, in linea di principio, elevare l'efficacia e l'efficienza della vigilanza sulla prevenzione dei reati.
Infatti, i poteri e gli obblighi attribuiti all'organo con funzione di controllo dalle norme di legge e regolamentari (alcuni dei quali anche con riferimento alle società controllate) possono comportare una maggiore incisività ed estensione della vigilanza, a prescindere dal contenuto dei modelli adottati ai sensi del D. Lgs. 231/2001 dalle singole società su base facoltativa e diversificata.

Si segnala tuttavia l'opportunità che sia assegnato all'organo di controllo il *budget* di spesa a carico dell'ente vigilato generalmente riconosciuto all'Organismo di Vigilanza, onde evitare che il rafforzamento ottenuto come sopra descritto possa poi essere compromesso da una interpretazione restrittiva degli artt. 2403-*bis*, ultimo comma, del codice civile e 151, terzo comma, del TUIF. Tali norme infatti prevedono che i sindaci, nell'espletamento di specifiche operazioni di ispezione e di controllo, possono avvalersi di dipendenti e ausiliari ma a proprie spese.

Procedura di allerta interna

Si condivide pienamente la scelta di far sì che le banche si dotino di una procedura di allerta interna, anche alla luce della prassi diversificata che in Italia si è consolidata con l'introduzione su base volontaria dei modelli organizzativi e di gestione ai sensi del D. Lgs. 231/01. Tale procedura in alcuni importanti paesi esteri è invece da tempo normativamente obbligatoria, tutelata ed incentivata (ad esempio, negli Stati Uniti, con il Sarbanes Oxley Act e il Dodd Frank Act).

Il recepimento da parte delle banche delle disposizioni in questione permetterà l'implementazione nel sistema bancario di un approccio sistematico ed omogeneo in materia, tale da garantire più efficacia allo strumento di controllo in questione.

Si segnala tuttavia l'opportunità che la procedura di allerta interna prevista nel Documento sia attivabile anche da parte di terzi. In effetti, il Documento sembra indicare che le segnalazioni possano essere effettuate solo dai dipendenti, salvo poi richiedere che le procedure di allerta identifichino i soggetti che le possono attivare.
Al riguardo, occorrerebbe a nostro avviso prevedere che dette segnalazioni, purché riferite a elementi o riscontri obiettivi e verificabili, possano provenire anche da soggetti estranei alla struttura aziendale.

Utilizzo della locuzione "Sistema dei controlli interni"

Il Documento contiene disposizioni in materia di "*sistema dei controlli interni, sistema informativo e continuità operativa delle banche e dei gruppi bancari*".
Gli scarni riferimenti normativi sul tema – precisamente, l'art. 2409-*octiesdecies* del codice civile, gli artt. 123-*bis*, co. 2, lett. b) e 149, co. 1, lett. c) del TUIF, l'art. 19 del D.Lgs. 39/2010 – nonché il Codice di Autodisciplina delle società quotate (nella sua versione più recente del dicembre 2011) fanno riferimento al "*sistema di controllo interno*".

La scelta di codesta Autorità di Vigilanza di utilizzare la locuzione al plurale pare derivare dal fatto che l'art. 53, comma 1, lett. d), del D.Lgs. 385/1993 ("TUB") attribuisce a Banca d'Italia il potere di emanare disposizioni di carattere generale aventi ad oggetto, tra l'altro, i "*controlli interni*", e così la disciplina regolamentare bancaria attualmente vigente.

Ci si chiede se, per chiarezza e uniformità terminologica, non sia preferibile ricorrere all'espressione al singolare prevista nel codice civile, nel TUIF e nel D.Lgs. 39/2010 e quindi utilizzare la locuzione "*sistema di controllo interno*".
Sotto un diverso profilo, considerata la centralità attribuita nel Documento al tema della gestione dei rischi e alla funzione di *risk management* – scelta che appare assolutamente condivisibile – si potrebbe valutare, in linea con quanto rinvenibile nel Codice di Autodisciplina (che nella sua versione più recente utilizza la definizione di "*Sistema di controllo interno e di gestione dei rischi*"), di aggiungere nella locuzione di "*Sistema dei controlli interni*" il riferimento alla "*gestione dei rischi*".

3. Osservazioni specifiche

3.1 Risk Appetite Framework

**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».**

Considerazioni generali

I concetti di *risk tolerance* e/o *risk appetite* sono specificamente richiamati in diverse parti del Documento; in particolare:
- tra le finalità generali del sistema dei controlli interni si individua «*il contenimento del rischio entro il limite massimo accettato ("tolleranza al rischio" o "appetito per il rischio")*» (Sezione I, Par. 6);
- l'organo con funzione di supervisione strategica « *definisce e identifica il livello di rischio accettato (c.d. "tolleranza al rischio" o "appetito per il rischio")*» (Sezione II, Par. 2);
- l'organo con funzione di gestione assicura «*… la coerenza tra il livello di rischio accettato, la pianificazione aziendale, le politiche di governo dei rischi e il processo di gestione dei rischi avuta anche presente l'evoluzione delle condizioni interne ed esterne in cui opera la banca*». (Sezione II, Par. 3).

ASSIREVI accoglie con favore l'obbligo che le nuove disposizioni pongono in capo all'organo con funzione di supervisione strategica di definire ed identificare il *risk appetite* e la *risk tolerance*. Questo obbligo, infatti, consente al sistema italiano di allinearsi alle *best practices* internazionali, riconoscendo peraltro che le principali banche italiane, anche alla luce della più recente regolamentazione nazionale ed internazionale, hanno iniziato a definire un proprio *risk appetite framework* ed a formalizzare la propensione al rischio.
Alla luce della recente esperienza, deve riconoscersi tuttavia come sussistano elementi di complessità tecnica e gestionale nella definizione del *risk appetite*, che risiedono principalmente nel:

- definire una propensione al rischio che sia effettivamente coerente (non solo compatibile) con gli indirizzi strategici, senza essere troppo generica;
- includere nella definizione del *risk appetite* un insieme di metriche, tra loro coerenti, che siano in grado di cogliere tutti i rischi a cui la banca è esposta;
- declinare il *risk appetite* in un sistema di procedure gestionali e di limiti operativi coerente sia nella sua formulazione che con riguardo alle strategie di rischio complessive della banca.

A conferma delle complessità applicative, le prassi seguite dalle banche internazionali - alcune delle quali riportano il proprio *risk appetite* nell'ambito dell'*Annual Report* - evidenziano una notevole differenziazione tra i vari operatori, che solo in parte risponde a differenze nelle scelte strategiche in materia di gestione del rischio.

E' proprio in considerazione dei diversi approcci, metodologici e di linguaggio esistenti, che l'Associazione auspica in via generale che l'introduzione di tale obbligo a livello regolamentare possa favorire una maggiore omogeneità metodologica e possa contribuire a far crescere una "cultura del rischio", attraverso lo sviluppo di una dialettica che stimoli l'assunzione dei rischi in modo consapevole e coerente con le più generali strategie aziendali.

L'Associazione auspica quindi che la nuova regolamentazione in materia di *risk appetite* abbia le seguenti caratteristiche:

- preveda un contenuto minimale per garantire una coerenza generale a livello di sistema e un *level playing field* regolamentare;
- la scelta delle metriche e, più in generale, la complessità del *risk appetite statement* rispondano al principio di proporzionalità. Per ragioni di coerenza complessiva dell'impianto regolamentare, ed essendo la propensione al rischio l'elemento di partenza per le strategie di gestione del rischio e del capitale, si ritiene opportuno che il principio di proporzionalità sia declinato in modo coerente con quanto previsto in materia di ICAAP;
- la propensione al rischio, almeno nei suoi elementi essenziali, sia comunicata non solo all'interno dell'organizzazione ma anche all'esterno. Infatti l'esplicitazione delle strategie di rischio può costituire un importante elemento che può consentire al mercato di valutare le scelte strategiche effettuate dai singoli operatori in rapporto ai rispettivi obiettivi e limiti di rischio.

Adozione di una tassonomia comune

Sebbene i termini *risk appetite* e *risk tolerance* siano spesso utilizzati come sinonimi, si riterrebbe opportuno delineare già a livello regolamentare almeno i seguenti concetti:

- *Risk appetite (propensione al rischio)*: la quantità e la tipologia di rischi che una banca è disposta ad assumere nel perseguimento dei suoi obiettivi di business. Il *risk appetite* è quindi concettualmente e praticamente separato dalla *risk capacity* o *risk bearing capacity;*
- *Risk capacity*: il massimo livello di rischio che la banca è tecnicamente in grado di assumere data la sua base di capitale, la sua posizione di liquidità attuale e prospettica e i vincoli regolamentari. La propensione al rischio è - di norma - inferiore alla capacità di assorbire i rischi;
- *Risk tolerance* è definita come la deviazione massima ritenuta accettabile dagli obiettivi di rischio stabiliti nel *risk appetite*.

Sebbene la relazione preliminare sull'analisi di impatto del Documento riconosca che l'espressione *risk tolerance/appetite* sia utilizzata in modo diverso dalle differenti istituzioni e autorità, la relazione stessa fornisce una tassonomia di riferimento secondo la quale la *risk tolerance* descrive i rischi assoluti effettivi che una banca ha assunto (ha quindi una logica ex-post), mentre il *risk appetite* descrive i rischi assoluti che un'istituzione è disposta ad assumere a priori. Pertanto, il concetto di *risk appetite* può assumere un duplice significato, vale a dire descrivere sia il livello *target* di rischio, sia il limite di rischio (ovvero un sistema di limiti di alto livello) che, se superato, comporta l'attivazione di specifiche procedure gestionali tese a riportare il livello di rischio entro i limiti massimi stabiliti.
Definita tale tassonomia, quindi, il *risk appetite* in senso stretto definisce un obiettivo di rischio, mentre la *risk tolerance* individua il limite oltre il quale sono necessarie specifiche azioni manageriali di "rientro".

In termini di *risk appetite statement*, ovvero della formalizzazione della propensione al rischio della banca, si ritiene opportuno che sia specificato sia il livello *target* sia il livello limite (ovvero la tolleranza massima alla deviazione rispetto agli obiettivi di rischio che la banca è disposta ad accettare e che attiva specifiche azioni di *remediation*). In tale ottica si suggerisce pertanto di integrare il ruolo dell'organo con funzione di supervisione strategica. Si potrebbe prevedere che quest'ultimo «*definisce e identifica il livello di rischio accettato, attraverso la definizione dell'"appetito per il rischio" che includa sia la quantità di rischio che la banca è disposta ad assumere nel perseguire i propri obiettivi di business, sia il livello limite che identifica una soglia oltre la quale devono essere attivate opportune azioni gestionali tese a riportare il livello di rischio entro i livelli massimi stabiliti*» (Documento, Sezione II, Par. 2).

Individuazione delle metriche utilizzate

Diversi studi hanno evidenziato come le prassi seguite dalle principali banche differiscano significativamente in materia di metriche utilizzate per la definizione della propria propensione al rischio. Sebbene sia spesso auspicato che le banche utilizzino un ampio numero di metriche e indicatori, si ritiene che, ai fini della definizione a livello regolamentare di un contenuto minimo , sia opportuno identificare un numero limitato di metriche. Il "contenuto minimale" del *risk appetite statement* non deve essere considerato come esaustivo; le banche potranno definire ulteriori metriche, articolate per singole tipologie di rischio.

ASSIREVI suggerisce quindi di definire un contenuto minimale del *risk appetite* che contenga almeno:

- obiettivi e limiti in termini di capitale (per i rischi quantificabili);
- obiettivi e limiti in tema di rischio di liquidità;
- obiettivi e limiti in termini di indicatori in grado di cogliere l'esposizione a determinate tipologie di rischio (per esempio, rischio reputazionale, rischio strategico e rischio di non conformità).

Si propone di seguito uno schema esemplificativo dei contenuti minimali e delle metriche del *risk appetite statement*:

	Classe 1	Classe 2	Classe 3
Capitale	Rating target oppure Rapporto tra AFR e capitale interno complessivo oppure CT1 e TCR Articolazione degli assorbimenti di capitale per tipologia di rischio (basati su metriche interne) per tutte le tipologie di rischio (minimo i rischi di Pillar 1) Articolazioni degli assorbimenti di capitale per business unit (basati su metriche interne) e, all'interno di queste, per tutte le tipologie di rischio (minimo i rischi di Pillar 1)	Ratio regolamentari: CT1 e TCR Quantità assoluta di patrimonio di vigilanza/ Capitale interno in eccesso rispetto al capitale interno complessivo	Ratio regolamentari: CT1 e TCR
Liquidità	LCR e NSRF oppure Espresso tramite modelli interni di misurazione del rischio di liquidità	LCR e NSRF oppure % di APL su totale attivo	LCR e NSRF

Nella tabella che segue sono elencate altre possibili metriche quantitative e qualitative utilizzate nella prassi dei principali operatori nazionali e internazionali[1]

Altri indicatori quantitativi	· Volatilità degli utili · RoE · Capitale economico per tipologia di rischio · Perdita attesa sul rischio di credito · Limiti al rischio di concentrazione · *Risk Weighted Asset* (RWA)
Elementi qualitativi	· *Compliance* regolamentare · Diversificazione delle di fonti di liquidità · Diversificazione di ricavo tra settori, linee di *business*,aree geografiche · *Market sentiment/ market confidence* nei confronti della banca · Rischio legale e reputazionale

Nel *risk appetite statement* è opportuno siano specificati sia i valori *target*, sia i valori limite che attivano specifiche azioni manageriali di rimedio.

3.2 Processo di gestione dei rischi

Definizioni e principi generali

Il Documento contiene specifiche disposizioni sul "*processo di gestione dei rischi*", di cui viene fornita anche una definizione di carattere generale, articolata attraverso prescrizioni più puntuali. Si riportano di seguito i principali riferimenti:

«"Processo di gestione dei rischi": l'insieme delle regole, delle procedure e delle risorse volte a identificare, misurare o valutare, monitorare, attenuare e comunicare ai livelli appropriati i rischi, come specificato nel par. 5» (Sezione I - Disposizioni preliminari e principi di carattere generale - Par. 3. – Definizioni);

«… il sistema dei controlli interni deve in generale:
- consentire di identificare, misurare o valutare, monitorare, attenuare e riportare ai livelli gerarchici appropriati adeguatamente tutti i rischi assunti o assumibili (strategico, credito, controparte, concentrazione, mercato, tasso di interesse, operativi, liquidità, reputazione, ecc.) nei diversi segmenti, a livello di portafoglio di impresa e di gruppo, cogliendone, in una logica integrata, anche le interrelazioni reciproche e con l'evoluzione del contesto esterno ("processo di gestione dei rischi").»

«A prescindere dalle strutture dove sono collocate, si possono individuare le seguenti tipologie di controllo:
- controlli di linea (c.d. "controlli di primo livello"), diretti ad assicurare il corretto svolgimento delle operazioni. Essi sono effettuati dalle stesse strutture operative (es. controlli di tipo gerarchico, sistematici e a campione) … Le strutture operative sono le prime responsabili del processo di gestione dei rischi: nel corso dell'operatività giornaliera tali strutture devono identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale in conformità con il processo di gestione dei rischi; esse devono

1 Vedasi The Institute of Risk Management (IRM), Risk Appetite and Tolerance – Guidance paper

assicurare il rispetto del livello di tolleranza al rischio stabilito e delle procedure in cui si articola il processo di gestione dei rischi
- controlli sui rischi e sulla conformità (c.d. "controlli di secondo livello"), che hanno l'obiettivo di assicurare, tra l'altro:
a) la corretta attuazione del processo di gestione dei rischi … » (Sezione I - Disposizioni preliminari e principi di carattere generale - Par. 6. – Principi generali).

Con riferimento all'insieme delle disposizioni sopra richiamate, di cui si condivide pienamente la sostanza, potrebbero essere utili alcuni affinamenti ai fini della loro corretta e puntuale applicazione. Si propone di:

a) Modificare la definizione di processo di gestione dei rischi specificando il contenuto del termine "risorse" che, avendo una portata di carattere generale, potrebbe rendere meno efficace il valore stesso della definizione fornita. Si potrebbe dunque fare riferimento a "*l'insieme delle regole, delle procedure, della strumentazione (anche informatica), delle attività di controllo e delle risorse umane volte a identificare, misurare o valutare, monitorare, attenuare e comunicare ai livelli appropriati i rischi, come specificato nel par. 5*";
b) In relazione alla precisazione sulle responsabilità delle strutture operative contenuta nella Sezione I - Disposizioni preliminari e principi di carattere generale - Par. 6. – Principi generali, sembrerebbe utile verificare l'allineamento con quanto indicato nel Documento in materia di "*Ruolo degli Organi Aziendali*" con particolare riferimento all'organo con funzione di gestione, responsabile di "*definire*" il Processo di gestione dei rischi e di "*assicurarne*" l'aderenza ai requisiti di cui alle Sezioni I e III (cfr. Documento, pag. 11). Al riguardo, si propone qui di seguito una possibile modifica al periodo in oggetto, tenendo conto anche di quanto indicato dalle "*EBA Guidelines on Internal Governance*" ove si prevede quanto segue: *«… In order to implement a strong internal control framework in all areas of the institution, the business and support units should be responsible in the first place for establishing and maintaining adequate internal control policies and procedures». La precisazione sulle responsabilità delle strutture operative potrebbe dunque indicare che «Le strutture operative (di business e di supporto) svolgono un ruolo fondamentale nel Processo di gestione dei rischi, il quale deve prevedere che nella loro operatività giornaliera tali strutture identificano, misurano o valutano, monitorano, attenuano e riportano i rischi derivanti dall'ordinaria attività aziendale; esse hanno la responsabilità di adottare e di mantenere politiche e procedure di controllo tali da assicurare il rispetto dei limiti (anche in termini di tolleranza al rischio stabilito) e delle regole in cui si articola il Processo di gestione dei rischi adottato dalla banca».*
c) Con riferimento alla previsione secondo cui i controlli sui rischi hanno l'obiettivo di "*assicurare*" la "*corretta attuazione del Processo di gestione dei rischi*" sembrerebbe potersi dedurre – stando al tenore letterale della formulazione - una responsabilità diretta delle funzioni di controllo di secondo livello nell'attuazione di tale processo. Nello stesso paragrafo, peraltro, si afferma che "*le strutture operative sono le prime responsabili del processo di gestione dei rischi"*. A parere dell'Associazione potrebbe evitare qualche dubbio interpretativo una formulazione alternativa che preveda che i controlli sui rischi e sulla conformità (c.d. "controlli di secondo livello") "*hanno l'obiettivo di verificare, tra l'altro: a) la corretta attuazione del processo di gestione dei rischi da parte di tutte le strutture della banca coinvolte*".

Approccio integrato alla gestione dei rischi

I principali riferimenti contenuti nel Documento al concetto di integrazione del processo di gestione sono individuabili nei seguenti passaggi:

«identificare, misurare o valutare, monitorare, attenuare e riportare ai livelli gerarchici appropriati adeguatamente tutti i rischi assunti o assumibili (strategico, credito, controparte, concentrazione, mercato, tasso di interesse, operativi, liquidità, reputazione, ecc.) nei diversi segmenti, a livello di portafoglio di impresa e di gruppo, cogliendone, in una logica integrata, anche le interrelazioni reciproche e con l'evoluzione del contesto esterno ("processo di gestione dei rischi")» (Sezione I - Disposizioni preliminari e principi di carattere generale – Par. 6 – Principi Generali);

«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. In tale ambito, deve essere in grado di individuare e valutare i fattori, inclusa la complessità della struttura organizzativa, da cui possono scaturire rischi per la banca» (*pag.* 10 Sezione II - Il ruolo degli organi aziendali – Par. 3 – Organo con funzione di gestione)*;*

«L'organo con funzione di gestione … agevola lo sviluppo e la diffusione a tutti i livelli di una cultura del rischio integrata in relazione alle diverse tipologie di rischi (di credito, di mercato, operativi, di liquidità, di concentrazione, di reputazione, di conformità, strategico, di modello ecc.) ed estesa a tutta la banca» (pag 11, Sezione II - Il ruolo degli organi aziendali – Par. 3 – Organo con funzione di gestione).

Questa Associazione condivide l'esigenza di favorire l'adozione di un approccio integrato alla gestione dei rischi che caratterizzano l'operatività bancaria; inoltre, apprezzabili risultano i riferimenti alla esigenza di cogliere le interrelazioni esistenti fra le diverse categorie di rischio.
A tal fine, tuttavia, si riterrebbe utile indicare specificatamente le caratteristiche di integrazione ritenute adeguate, anche in una logica di mera esemplificazione minimale e ferma restando l'autonomia organizzativa delle banche.

Inoltre, nell'ambito dell'analisi delle responsabilità e del ruolo dell'organo con funzione di supervisione strategica non sembrano riscontrarsi riferimenti all'esigenza di un approccio integrato alla gestione dei rischi, che invece ci pare dovrebbe essere favorito e disegnato proprio dal predetto organo.
Tali modifiche sembrano poter rafforzare il contenuto delle disposizioni relative all'adozione di un approccio integrato alla gestione dei rischi e paiono del tutto coerenti con il principio definito da codesta Autorità di Vigilanza in base al quale il "*sistema dei controlli interni ha rilievo strategico*".

In relazione alle osservazioni sopra formulate sembrerebbe opportuno:

a) integrare il Par. 6 – Principi generali con l'introduzione di una specifica frase indicante le caratteristiche di integrazione ritenute adeguate. Si potrebbe, ad esempio, inserire un passaggio del seguente tenore: «*Un governo adeguato di tutti i rischi aziendali implica l'adozione di un Processo di gestione dei rischi che sia efficacemente integrato. Sono considerati parametri di integrazione i seguenti elementi, riportati a titolo esemplificativo e non esaustivo: la diffusione di un linguaggio comune nella gestione dei rischi a tutti i livelli della banca; l'adozione di metodi e strumenti di rilevazione e valutazione tra di loro coerenti (ad es.: unica tassonomia dei processi; unica mappa dei rischi); la definizione di modelli di reportistica trasversali alle diverse tipologie di rischio, al fine di favorirne la comprensione e la corretta valutazione; ancora, sotto il profilo della operatività delle funzioni coinvolte nel Processo di gestione del rischio, l'individuazione di momenti formalizzati di coordinamento ai fini della pianificazione delle rispettive attività sulla base dei rischi in essere; la previsione di flussi informativi su base continuativa tra le diverse funzioni in relazione ai risultati delle attività di controllo di propria pertinenza; la condivisione nella individuazione delle azioni di rimedio*».
b) Con riferimento alla Sezione II - Il ruolo degli organi aziendali, potrebbe essere utile integrare le previsioni secondo cui l'organo con funzione di supervisione strategica "*definisce gli indirizzi strategici e le politiche di governo dei rischi"* , stabilendo che detto organo, nella definizione del livello di rischio accettato e nelle politiche di governo dei rischi, adotta una visione integrata dei rischi in relazione ai diversi ambiti di attività della banca. Inoltre, con riferimento alla definizione da parte dell'organo con supervisione strategica delle linee di indirizzo del sistema dei controlli interni, si potrebbe richiedere che detto organo individui altresì il necessario sviluppo di fattori, strutturali ed operativi, di integrazione tra le funzioni di controllo dei rischi e le altre strutture della banca.

Operazioni di maggiore rilievo

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

In relazione alle operazioni di maggior rilevo da sottoporre a valutazione preventiva da parte della funzione di *risk management*, i riferimenti contenuti nel Documento sono i seguenti.

L'organo con funzione di supervisione strategica definisce «*… 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*» (Sezione II - Il ruolo degli organi aziendali – Par. 2 – Organo con funzione di supervisione strategica).

L'organo con funzione 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 (cfr. Sezione III, par. 3.3.); di tali operazioni informa l'organo con funzione di supervisione strategica e l'organo con funzione di controllo*» (Sezione II - Il ruolo degli organi aziendali – Par. 3 – Organo con funzione di gestione).

La funzione di controllo dei rischi «*…dà pareri preventivi sulla coerenza con la politica di governo dei rischi delle operazioni di maggiore rilievo*». (Sezione III - Funzioni aziendali di

controllo – Par. 3 – Requisiti specifici delle funzioni aziendali di controllo – 3.3. Funzione di controllo dei rischi).

L'insieme delle disposizioni richiamate evidenziano taluni aspetti di struttura e di processo su cui questa Associazione vuole richiamare preliminarmente l'attenzione. In primo luogo, tenuto anche conto delle valutazioni espresse da codesta Autorità, si ritiene che i criteri per l'individuazione delle "*operazioni di maggiore rilievo*" debbano fare riferimento ai limiti di "*risk tolerance*" fissati dall'organo con funzione di supervisione strategica. Pertanto, si ritiene che rientrino tra le operazioni da sottoporre al vaglio preventivo della funzione di controllo del rischio quelle che comportano il superamento (o anche solo l'avvicinarsi) delle (o alle) soglie quali-quantitative di rischio fissate in sede di identificazione e definizione del "*livello di rischio accettato*".

Al riguardo, si ritiene opportuno individuare, anche solo in via esemplificativa, talune operazioni che sono rilevanti per il loro impatto potenziale (soprattutto in termini reputazionali e/o strategici) sul profilo di rischio.
A tal fine varrebbe la pena esplicitare i seguenti possibili parametri generali di riferimento, che dovrebbero essere valutati a prescindere dai volumi dell'operazione medesima e dall'impatto previsto sui coefficienti patrimoniali:

- controparte/i coinvolta/e. Le operazioni con controparti aventi sede in una giurisdizione "non trasparente", ovvero la cui struttura societaria presenta elementi di "opacità" e/o di complessità, ovvero che possano dar luogo a situazioni di conflitto di interesse (perché la controparte è un soggetto collegato, oppure è un cliente rilevante) oppure appartengono a specifiche categorie sensibili (aziende della PA);
- tipologia dell'operazione. Le operazioni che, pur nell'ambito della operatività della banca, implichino delle specifiche deroghe a significativi *standard* operativi e contrattuali (ad esempio, operazioni di finanziamento che implichino la definizione di accordi contrattuali diversi da quelli adottati in via generale dalla banca; operazioni di investimento effettuate attraverso il ricorso a SPV o altre strutture societarie complesse);
- coerenza con gli indirizzi strategici della banca. Ogni iniziativa che non sia direttamente ed immediatamente correlabile agli indirizzi strategici fissati dagli organi aziendali (ad es. segmenti di clientela, attivazione di canali distributivi, accordi con soggetti terzi).

In via esemplificativa quindi si ritiene che i criteri da considerare ai fini della rilevanza delle operazioni possano essere individuati nei seguenti:

Impatto sui limiti di tolleranza al rischio	Controparte	Tipologia Operazione	Coerenza con gli indirizzi strategici
Assorbimento del capitale superiore allo xx% del PdV è Rilevante *o* **Superamento Limiti è Rilevante** *o* **Approssimarsi Limiti (-x%) è Rilevante**	**Giurisdizione non trasparente è Rilevante** e/o **Gruppo non trasparente è Rilevante** **e/o** **Connessione/conflitti di interesse è Rilevante**	**Deroga a clausole standard è Rilevante** e/o **Ricorso a strutture societarie complesse è Rilevante** e/o **Operazioni di mercato eseguite con controparti (assenza di meccanismi centralizzati di compensazione e garanzia) è Rilevante**	Da declinare in funzione alla articolazione dei singoli piani strategici

Ove le "*operazioni rilevanti*" siano soggette a procedure deliberative appositamente previste da normative specifiche (ad es. operazioni con parti correlate, acquisto di partecipazioni rilevanti, conflitti di interesse), la previsione del parere preventivo da parte del responsabile del *risk management* si aggiunge alle previste procedure ed in ogni caso non deve essere tale da modificarne o alterarne gli specifici presidi.

Con riferimento al processo di individuazione delle operazioni di maggiore rilievo, si ritiene sussista qualche incertezza in relazione al soggetto/organo competente. Non sembrerebbe chiaro nello specifico chi identifica le operazioni di maggiore rilievo. A tal proposito si riterrebbe utile modificare quanto indicato al Par. 3 della Sezione II specificando che l'organo con funzione di gestione «*individua le operazioni di maggiore rilievo in funzione dei criteri fissati dall'organo di supervisione strategica e le sottopone al parere della funzione di controllo dei rischi prima della loro effettuazione. In caso di parere negativo, l'organo esamina tali operazioni e, se del caso, le autorizza (cfr. Sezione III, par. 3.3.); di tutte le operazioni individuate informa l'organo con funzione di supervisione strategica e l'organo con funzione di controllo*».
Inoltre, considerata anche l'ampiezza delle problematiche che le operazioni di maggiore rilievo possono comportare, parrebbe opportuno integrare la previsione secondo cui la funzione di controllo dei rischi «*dà pareri preventivi sulla coerenza con la politica di governo dei rischi delle operazioni di maggiore rilievo*», inserendo il seguente periodo finale «*eventualmente acquisendo, in funzione della natura della operazione, il parere di altre funzioni interne coinvolte nel processo di gestione dei rischi (ad es. funzione di compliance, funzione ICT)*».

Funzione di Controllo dei rischi

Si condivide in generale l'impostazione adottata dall'Autorità in relazione al ruolo che la funzione di controllo dei rischi dovrebbe assumere nella banca. Valgono a tal fine non solo la definizione puntuale dei compiti della funzione contenuta nel Documento ma anche il rilievo che l'Autorità attribuisce alla figura del CRO nell'ambito della Relazione Preliminare di Impatto.
La puntuale declinazione dei compiti della funzione di controllo dei rischi potrebbe essere arricchita, anche in un'ottica di "logica integrata", con una specifica analisi del ruolo della funzione stessa in relazione alle principali categorie di rischio che caratterizzano l'operatività della banca.

Si ritiene in particolare che specifiche indicazioni possano essere fornite per alcune categorie di rischio, per le quali significativa appare l'esigenza di una integrazione con altre funzioni di gestione/controllo dei rischi. Potrebbe essere opportuno, pertanto, arricchire l'elencazione dei compiti delle funzioni di controllo dei rischi con l'esplicitazione di alcune attribuzioni che risulterebbero al momento solo sottese all'impianto del Documento, quali ad esempio:

- la definizione di metriche comuni di valutazione dei rischi operativi, coerenti con le politiche di governo dei rischi, coordinandosi con le funzioni di controllo di conformità e le funzioni ICT della banca;
- la definizione di modalità di valutazione e controllo dei rischi reputazionali, coordinandosi con le funzioni della banca che in primo luogo sono chiamate a gestire tali tipologie di rischio (funzioni di comunicazione, investor relations, ecc.);
- il supporto ai competenti organi della banca ai fini della valutazione del rischio strategico, tenuto anche conto di variabili esogene a valenza significativa (ad es. evoluzione normativa in specifici settori di business; variabili macroeconomiche per aree geografiche; tendenze demografiche; riforme ad impatto sistemico);
- la verifica sulla coerenza dei sistemi di misurazione e controllo dei rischi con i processi e le metodologie di valutazione, anche a fini contabili, delle attività aziendali, coordinandosi con le strutture aziendali a vario titolo coinvolte nei suddetti processi in coerenza con i principi generali di cui al Par. 6, Sez. 1, del Documento.

3.3 Rischio informatico

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

Considerazioni generali

ASSIREVI accoglie con favore le novità introdotte dal Documento con riguardo al complessivo assetto dei sistemi informativi della banca. Si ritiene infatti che la nuova disciplina consenta di uniformare l'organizzazione, le responsabilità ed il modello del processo di gestione del rischio informatico nel più ampio sistema di *governance* della banca.
Inoltre, la formalizzazione del livello di tolleranza al rischio informatico garantisce la completezza del relativo processo di gestione, in coerenza con i processi di gestione delle altre tipologie di rischio.

Integrazione del processo di gestione del rischio informatico e la gestione dei rischi operativi

Il modello di valutazione dei rischi informatici può/deve innestarsi all'interno di due fasi distinte del complessivo processo di gestione dei rischi operativi:

- la misurazione dei rischi operativi attraverso la raccolta di dati interni;
- la misurazione delle perdite potenziali attraverso analisi di scenario.

Una perdita associata ad un rischio operativo può essere ricondotta ad uno o più fattori di rischio; tali fattori possono essere associati a risorse umane, a sistemi informativi, a processi o ad eventi esterni (criminalità/situazione socio-politica/eventi ambientali). Una stima accurata dell'incidenza dei singoli fattori di rischio sulle perdite pregresse concorre a individuare quindi le aree maggiormente critiche e a identificare misure correttive per ridurre il rischio operativo complessivo. Maggiore è il livello di accuratezza e dettaglio con cui si riesce a determinare l'incidenza relativa di ogni singolo fattore di rischio, maggiore è la possibilità di utilizzare i dati di consuntivazione delle perdite per indirizzare le attività di gestione del rischio informatico.

Tanto premesso, si formulano le seguenti osservazioni sulla integrazione del rischio informatico nel più ampio ambito dei rischi operativi:

- la valutazione del rischio informatico, ancorché basata anche su elementi di natura soggettiva "*secondo una metodologia definita dall'organo di gestione"* (Sez. III, La gestione del rischio informatico), dovrebbe essere comunque coerente con i dati storici relativi alle perdite operative registrate in relazione alle diverse risorse informatiche, tenuto anche conto dell'incidenza degli altri fattori di rischio. A tal proposito, nello sviluppo della metodologia generale di riferimento e/o nella raccolta delle valutazioni sul rischio da parte dell'"utente responsabile", pare opportuno prevedere almeno un raccordo con la funzione aziendale incaricata della rilevazione dei dati di perdita e della valutazione dei rischi operativi (*operational risk management*). Peraltro, tale raccordo favorirebbe una maggiore precisione anche nella successiva fase di accettazione o mitigazione del rischio informatico, rispetto ai possibili piani di rientro. Anche laddove non esistano o non siano disponibili adeguate serie storiche degli incidenti - caso frequente per gli incidenti più gravi di norma molto rari - la valutazione espressa dall'"utente responsabile" dovrebbe comunque essere supportata dalle funzioni di *operational risk*, attraverso opportuni

benchmark esterni, che comprendano i processi e le tecnologie di supporto e che siano in grado di comprovare che il livello di controllo aziendale è almeno allineato agli *standard* di sistema;

- nello scenario di misurazione delle perdite potenziali la componente di valutazione del rischio informatico rappresenta, nella prassi, un fattore analizzato nell'ambito del processo di *risk self assessment*. Inoltre, la valutazione del rischio informatico è effettuata a livello aggregato, considerando dunque il livello di applicazione delle contromisure di sicurezza generalmente nel contesto IT, e di conseguenza individuando un'esposizione complessiva a determinati rischi operativi associati. Anche sul punto è opportuno che il livello di dettaglio attraverso il quale viene effettuata la valutazione del rischio informatico sia il più possibile coerente con l'articolazione dei rischi operativi, consentendo in tal modo di raccordare in maniera integrata l'impatto e il monitoraggio / mitigazione del rischio informatico all'interno del rischio tollerato a livello aziendale.

Ancorché la componente informatica sia solitamente associata ai rischi operativi, è auspicabile ipotizzare che l'analisi del rischio informatico possa essere associata ad altre tipologie di rischio, quali ad esempio:

- rischio strategico;
- rischio di non conformità rispetto a norme o regolamenti esterni;
- rischio reputazionale.

Tali interrelazioni, unitamente ad un adeguato livello di accuratezza della rilevazione dei fattori di rischio, favorirebbero da un lato una più puntuale fissazione del *risk appetite* e, dall'altro, la definizione di un processo di controllo dei rischi effettivamente integrato.

In relazione a quanto sopra si ritiene quindi di poter individuare – quali spunti atti a migliorare il processo di gestione del rischio informatico in un'ottica di integrazione con tutti i rischi della banca – i seguenti interventi, sia di natura metodologica, sia di processo:

- Favorire l'adozione di metodologie di analisi dei rischi informatici che siano integrate con la valutazione e l'analisi dei rischi operativi, al fine di mappare con maggiore accuratezza i fattori di rischio informatico, le possibili minacce e i relativi impatti, indirizzando di conseguenza gli interventi e le contromisure di mitigazione. Si riterrebbe opportuno, ad esempio, prevedere che l'organo con funzione di supervisione strategica «*approva il quadro di riferimento organizzativo e metodologico per l'analisi del rischio informatico, volto ad assicurare che tale categoria di rischio sia regolarmente identificata, valutata e trattata nei vari settori operativi, secondo criteri uniformi rispetto all'universo dei rischi operativi che ne evidenzino le interrelazioni, nonché opportunamente aggregata e comunicata attraverso i livelli di management e gli organi aziendali*».
- Delineare modelli organizzativi e di processo atti ad agevolare una valutazione maggiormente completa del rischio informatico, coerente con i dati di perdita ovvero con eventuali *benchmark* esterni (ove i dati interni non ci siano o siano non completi). Risulta in tal caso opportuno prevedere che i modelli di analisi e di definizione del *risk appetite* in ambito IT siano integrati con le metriche dell'*operational risk appetite framework* della banca.
- Favorire l'introduzione di un modello di *reporting* sul rischio IT, condiviso ad esempio tra le funzioni di *operational risk* e *IT security*, per la consuntivazione del rischio informatico, coerentemente con il modello di analisi dei rischi operativi, anche nell'ottica di migliorare l'esame e l'indirizzo delle strategie e governo delle infrastrutture IT.

Data Governance

ASSIREVI attribuisce particolare valenza all'introduzione dell'obbligo di definire uno "*standard aziendale di data governance, che individua ruoli e responsabilità delle funzioni coinvolte nel trattamento delle informazioni nonché le misure atte a garantire la qualità dei dati, sia operativi che gestionali"*. Tale *standard* è approvato dall'organo con funzione di gestione.

Proprio in considerazione dell'importanza di tale previsione, ad avviso di ASSIREVI potrebbero essere utili alcuni affinamenti:

a) Precisare ed integrare il contenuto minimo dello *standard*, prevedendo che tale documento *«individua ruoli e responsabilità delle funzioni coinvolte nel trattamento (acquisizione, elaborazione, validazione ed utilizzo) dei dati, classifica i dati, sia operativi che gestionali, in funzione della loro rilevanza nel sistema informativo aziendale, identifica, in funzione della rilevanza, le misure atte a garantirne la qualità (in termini di completezza e accuratezza)»*.
b) Con riferimento alla previsione contenuta nella nota n. 25, potrebbe essere utile un maggior dettaglio del contenuto, anche in relazione alle responsabilità organizzative ad oggi in essere. In particolare i dati "*rilevanti*" di cui trattasi (informazione al mercato, segnalazioni all'OdV, valutazione dei rischi) sono di norma il risultato di un processo di elaborazione, validazione e controllo che coinvolge diversi attori, con responsabilità articolate e fissate dalla normativa di riferimento. L'obbligo, per le banche appartenenti alle macro-categorie 1 e 2, di individuare uno o più responsabili della qualità dei dati "rilevanti", pertanto, potrebbe apparire ridondante rispetto all'obbligo di "*definire ruoli e responsabilità delle funzioni coinvolte nel trattamento*" dei dati. Al contrario, potrebbe essere più utile prevedere che, per alcuni dati "rilevanti", sia stabilita una responsabilità in termini di validazione della qualità, consistente nella attestazione di avere eseguito tutti i controlli previsti (in termini di completezza ed accuratezza) prima di rendere disponibili i dati ai fini della informativa "rilevante".

Altri commenti specifici in materia di ICT

In relazione alle ulteriori disposizioni relative al rischio informatico, ASSIREVI propone di seguito alcune considerazioni puntuali.
In particolare:

a) *"… con riguardo al contenimento del rischio operativo, il regolare svolgimento dei processi interni e dei servizi forniti alla clientela, l'integrità, la riservatezza e la disponibilità delle informazioni trattate nonché la sicurezza dei valori custoditi fanno affidamento in misura rilevante sull'adeguatezza e funzionalità dei controlli automatizzati"* (Sezione I - Disposizioni di carattere generale - 1. Premessa – Pag. 44).
   In generale i controlli automatizzati non sono adeguatamente documentati, rendendone così più difficoltosa la gestione e la possibilità di verifica efficiente ed efficace da parte delle strutture di controllo interno ed esterno. Ad avviso di questa Associazione sarebbe opportuno, almeno per i controlli chiave di processi critici, l'utilizzo di uno *standard* aziendale di *governance* dei controlli automatizzati (del tipo di quello utilizzato per i dati) che includa le politiche di documentazione e gestione del controllo e il riferimento al relativo rischio informatico.
b) *"…le procedure per lo svolgimento delle operazioni critiche, con riguardo ai principi del minimo privilegio e della segregazione dei compiti (ad esempio specifiche procedure di abilitazione e di autenticazione, controlli di tipo four eyes , o di verifica giornaliera ex-post)";* (Sezione IV - Il sistema di gestione della sicurezza informatica 1. Policy di sicurezza - 2. La sicurezza dei dati e il controllo degli accessi – Pag. 53).

Secondo Assirevi l'effettuazione di operazioni critiche da parte di personale tecnico, ovvero l'utilizzo di funzionalità dispositive al di fuori della normale operatività, dovrebbero essere tracciate in modo automatico, compatibilmente con le possibilità tecnologiche, in quanto spesso dette operazioni hanno un carattere di urgenza difficilmente compatibile con l'esecuzione di una procedura manuale di richiesta, approvazione e documentazione.

c) l'organo con funzioni di supervisione strategica"… *è informato con cadenza almeno annuale 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"* (Sezione II - Governo e organizzazione dell'ICT Compiti dell'organo con funzione di supervisione strategica – Pag. 47).
L'Associazione ritiene opportuna, secondo un principio di proporzionalità, l'adozione di uno *standard* aziendale di valutazione dei servizi erogati dal sistema informativo che utilizzi sia parametri di *user satisfaction,* sia parametri oggettivi di effettivo utilizzo delle risorse informatiche a supporto dei diversi processi aziendali.

3.4 Modelli di cloud computing

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.

L'adozione di modelli di *cloud computing* si concretizza nell'esternalizzazione dei servizi ICT a fornitori che erogano i servizi stessi secondo lo schema denominato appunto *cloud computing*. Rimane quindi fondamentale il rispetto, anche in questo caso, di tutte le disposizioni previste per l'esternalizzazione di servizi, specie quelle relative alla scelta del fornitore stesso.
Si sottolinea, inoltre, come la formalizzazione degli accordi con i fornitori e la definizione ex ante dei presidi necessari a monitorare tali sistemi sia fondamentale all'interno dell'intero processo e debba prevedere il coinvolgimento diretto delle funzioni aziendali responsabili citate nel Documento.
Ciò detto, l'adozione di modelli di *cloud computing* nelle forme del *community cloud* e del *public cloud* comporta, ancor più di un affidamento in *outsourcing* tradizionale, la necessità di definire alcuni aspetti chiave nei contratti. Ciò, a causa dei maggiori rischi potenziali riconducibili prevalentemente all'utilizzo da parte di una pluralità , più o meno ristretta a seconda che si tratti di *community* o *pubblic cloud*, di organizzazioni clienti che hanno accesso al servizio medesimo.

Tra questi aspetti riteniamo opportuno segnalare:
a) la definizione delle politiche di *lock-in* necessarie per garantire:
- La completezza dei dati trasferiti al momento del conferimento dell'incarico;
- La possibilità di ottenere, al momento della cessazione del contratto, tutti i dati dell'intermediario e la loro disponibilità in un formato idoneo a consentirne la portabilità;

b) la definizione delle modalità e dei tempi di eliminazione in via definitiva di tutti i dati dai supporti di memorizzazione e di *back up* del fornitore, da effettuare alla conclusione del contratto, e le relative garanzie ottenute dal fornitore stesso;
c) la definizione preventiva delle procedure di *back up* in termini di frequenza, modalità di archiviazione, responsabilità, tempi di conservazione dei dati e tempo di ripristino in caso di *disaster recovery*. Ad esempio l'effettuazione di *back up* differenziali a distanza di brevi intervalli temporali permette il recupero veloce dei dati modificati dall'ultimo *back up* completo;

d) la definizione di un *uptime* adeguato ed i relativi sistemi di garanzia di tale servizio (continuità della fornitura energetica, utilizzo di gruppi di continuità, gruppi elettrogeni, servizi ridondati, stabilità della connettività), dato che l'utilizzo di sistemi in *cloud computing* si basa sulla fruizione delle risorse informatiche attraverso la rete);
e) i sistemi di *disaster recovery* per il tempestivo ripristino del servizio in caso di emergenza: ad esempio richiedere l'utilizzo di *data center* ubicati in aree geografiche diversificate su cui far affidamento.

In qualsiasi sistema in cui vi sia un trasferimento di dati verso l'esterno esiste un rischio legato alla sicurezza dei dati. La definizione di procedure interne e con il fornitore volte a garantire la sicurezza dei dati riveste un ruolo basilare. Come evidenziato anche dal Garante per la protezione dei dati personali nel documento "*Cloud Computing: indicazioni per l'utilizzo consapevole dei servizi*", gli aspetti che necessitano di specifica attenzione sono:

- i meccanismi di sicurezza adottati dal *service provider* in termini di accesso fisico e terminale ai *server* dell'infrastruttura *cloud* ed ottenimento dall'*outsourcer* di un elenco contenente i nominativi, i *log* di accesso e le ACL[2] di ciascun dipendente che ha accesso terminale alle macchine. In questo modo l'intermediario potrebbe creare una procedura di controllo volta al monitoraggio dei terzi che hanno accesso ai dati gestiti in modalità *cloud*.
- La previsione di adeguati presidi in caso di necessità di accesso fisico al locale dei *data center* da parte dei tecnici e di eventuali terzi coinvolti nella gestione del *cloud* (accesso con *badge*, videosorveglianza dei locali, accesso supervisionato da parte del personale del *data center* nel caso di utilizzo di *data center* esterni al fornitore, ecc.).
- Il servizio prescelto potrebbe essere il risultato finale di una catena di servizi; di conseguenza anche l'affidamento da parte del fornitore di incarichi a terzi che intervengano nell'intero processo che interessa il modello di *cloud computing* prescelto deve essere specificatamente normato in sede contrattuale.
- La possibilità che abbiano accesso al medesimo sistema di *cloud computing* soggetti con interessi ed esigenze differenti o addirittura contrastanti o in concorrenza.
- Alcuni sistemi per garantire la confidenzialità dei dati, quali:
    - Utilizzo di connessioni cifrate ed utilizzo di protocolli sicuri nella fase di trasmissione dati (https/ssl);
    - Adozione di meccanismi di identificazione dei soggetti autorizzati all'accesso (es. limitare la possibilità di collegamento per ciascun utente da un solo dispositivo alla volta; accesso con "*one time password*"; prevedere una complessità minima delle *password*);
    - Conservazione dei dati in forma cifrata sui sistemi del fornitore del servizio.

Ad avviso di Assirevi sarebbe inoltre opportuno enfatizzare l'intervento delle funzioni aziendali di controllo nel monitoraggio dei rapporti con il fornitore e nello svolgimento di verifiche specifiche di *compliance* e di *internal audit* nel corso dell'intera durata del rapporto contrattuale mirate a verificare il rispetto delle *policy* aziendali preventivamente definite e condivise con l'*outsourcer*.

2 ACL - Access Control List: permessi di lettura e scrittura su file system.

4. Conclusioni

In sintesi, nel ribadire il pieno apprezzamento per l'iniziativa di codesta Autorità di Vigilanza, ASSIREVI intende sottolineare come talune novità delle nuove disposizioni rappresentino una rilevante evoluzione del quadro normativo di riferimento e un fattore di cambiamento atto ad incidere in modo significativo sul sistema bancario nazionale.
In primo luogo, si ritiene che particolare valore aggiunto sia riscontrabile nel rafforzamento del legame tra gli organi aziendali e le funzioni aziendali di controllo, rafforzamento che consente di superare *"la riconosciuta incoerenza tra i rischi che l'intermediario effettivamente assumeva e quelli percepiti dagli organi decisionali dell'intermediario stesso"* (cfr. Relazione al Documento). Sotto tale profilo assume particolare valenza proprio la corretta declinazione del *risk appetite*, in relazione alla quale questa Associazione ha fornito nella presente risposta alcuni contributi.

Un altro aspetto meritevole di attenzione è la riconosciuta esigenza di definire modalità di coordinamento e raccordo tra le diverse funzioni di controllo (ai diversi livelli), per favorirne le possibili sinergie e per rafforzarne l'efficacia. Si ritiene che tali obiettivi siano perseguibili anche favorendo una maggiore "integrazione" tra le funzioni di controllo dei rischi (o di secondo livello), individuando in via generale alcuni requisiti di integrazione atti, a parere di questa Associazione, a rendere ancora più efficace il processo di gestione dei rischi.

Infine, si ritiene che la variabile informatica abbia una valenza strategica nelle banche e che le prescrizioni relative al governo ed alla gestione delle risorse informatiche siano correttamente indirizzate. Tuttavia, preme ribadire come tali previsioni possano avere una maggiore efficacia se inserite in un sistema di governo dei rischi effettivamente integrato (in termini di regole, processi, procedure e metodologie). In tale ambito, anche considerata la recente evoluzione del sistema finanziario internazionale, appare particolarmente rilevante la previsione di uno *standard* di *data governance* a livello di banca e di gruppo, per il quale si suggerisce un maggior dettaglio in termini di contenuto minimale.

Milano, 31 ottobre 2012