Documento di consultazione della Banca d'Italia
"*Disposizioni di vigilanza in materia di sistema dei controlli interni, sistema informativo e continuità operativa*"

Sommario

Premessa

Le disposizioni in consultazione concernono la nuova disciplina di vigilanza prudenziale in materia di sistema dei controlli interni, sistema informativo e continuità operativa.
Lo schema definisce il quadro di principi e regole cui deve ispirarsi il sistema dei controlli interni e costituisce la cornice di riferimento per le disposizioni in materia di controlli definite nell'ambito di altri specifici contesti disciplinari.
Nel documento vengono, tra l'altro, precisati:

- i principi generali del sistema dei controlli interni;
- il ruolo degli organi aziendali;
- l'istituzione e i compiti delle funzioni aziendali di controllo;
- i presidi richiesti riguardo ai rischi di esternalizzazione delle funzioni aziendali e le condizioni per esternalizzare funzioni aziendali importanti o di controllo ;
- il sistema dei controlli nei gruppi bancari;
- i requisiti di base in materia di *governance* e\\ organizzazione dell'ICT, gestione del rischio informatico, sicurezza informatica, sistema di gestione dei dati, esternalizzazione di sistemi e servizi.

A tale riguardo, in via preliminare, la scrivente Federcasse, nel manifestare il suo apprezzamento per le modalità di consultazione adottate con riferimento alla materia in oggetto, ringrazia altresì per la possibilità di esprimere opinioni e commenti sul tema.

Nel merito delle proposte Disposizioni, la scrivente rappresenta altresì la condivisione, in via generale, delle posizioni elaborate sul Provvedimento da parte dell'Associazione Bancaria Italiana cui si rinvia per quanto non qui commentato.

A integrazione delle citate posizioni, preliminarmente si osserva come, nell'adeguamento a un sempre più complesso e articolato quadro di riferimento normativo, un problema specifico delle piccole banche sia l'effetto, ovviamente non intenzionale, che nuovi riferimenti di vigilanza possono indurre in termini di aumento dei costi di *compliance*. Laddove, a titolo esemplificativo, l'adeguamento a una determinata disposizione richieda l'individuazione di una risorsa dedicata o l'attribuzione di nuove responsabilità e attività a risorse esistenti, l'impatto in termini di incremento del costo del personale incide, in proporzione, in misura significativamente maggiore sulle aziende di minori dimensioni. L'aumento degli oneri per la necessità di adeguarsi alle norme può generare, quindi, la rincorsa a una sorta di economie di scala artificiali, di natura esclusivamente regolamentare, che in assenza di correttivi adeguati potrebbero determinare una crescita dimensionale non funzione di una consapevole strategia ma conseguenza non intenzionale dei crescenti oneri di *compliance*.

Ciò posto, auspicando un'applicazione proporzionale della disciplina in oggetto alle banche di minori dimensioni e complessità operativa, nel merito dei contenuti del documento di

consultazione si formulano, con specifico riferimento alla prospettiva delle Banche di Credito Cooperativo - Casse Rurali (BCC-CR) e degli altri Enti di Categoria, le seguenti osservazioni che la scrivente Federcasse sottopone all'attenzione di Codesta Banca d'Italia.

Sintesi dei principali profili critici per il Credito Cooperativo

1. Tempistica di adozione del nuovo quadro di riferimento

Il documento di consultazione non precisa i termini di vigenza delle nuove disposizioni.

Si evidenzia che diversi profili notevolmente innovativi potrebbero risultare di importante impatto strategico, organizzativo, procedurale e applicativo. Si ritiene pertanto necessario, perlomeno con riguardo ai contenuti che innovano il quadro dispositivo vigente, prevedere un'entrata in vigore opportunamente dilazionata, tale da permettere agli intermediari di operare con adeguata riflessione le **scelte strategiche per l'adeguamento**, attuare un'**attenta pianificazione degli interventi** individuati e la messa in opera delle soluzioni di adeguamento **assicurandone efficacia ed efficienza**.
Tale periodo dovrebbe tenere conto anche **della presumibile necessità di interventi statutari per l'adeguamento a talune disposizioni**.

In relazione alla stima dei tempi di implementazione ritenuti necessari con riguardo agli interventi organizzativo/procedurali, alle attività e ai presidi individuati come necessari per un compiuto adeguamento, si ritiene che questi dipendano oltre che dalla misura dei gap registrati, dall'eventuale accoglimento di alcune delle criticità evidenziate nel presente documento.
Anche per tale ragione, non risulta possibile esprimere una stima compiuta dei tempi ritenuti necessari per l'adeguamento alle disposizioni in commento, anche se si ritiene che per alcune innovazioni di particolare impatto questi, tenuto anche conto della necessità di porre in essere soluzioni integrate a livello di Categoria, potrebbero superare i 18 mesi.
Si ritiene, comunque, auspicabile che, con riguardo ai contenuti di maggiore complessità e impatto, venga mantenuta una ragionevole flessibilità dei tempi disponibili per l'adeguamento, anche sulla base di una costante interlocuzione che permetta alle competenti strutture della Banca d'Italia di acquisire e verificare il piano degli interventi definiti e la relativa attuazione.

Ferme le valutazioni sul merito di talune delle previsioni richiamate, si evidenziano nel seguito, a titolo esemplificativo, alcuni tra i principali contenuti innovativi relativamente ai quali si ritiene imprescindibile la definizione di un congruo periodo di tempo per l'adeguamento:

- ampliamento del perimetro di competenza della *compliance* con inclusione obbligatoria nello stesso delle norme fiscali, in un'accezione, peraltro, estesa anche ai rischi derivanti

dall'eventuale coinvolgimento in operazioni fiscalmente irregolari poste in essere dalla clientela;

- obbligo di definire un sistema di allerta interna per permettere la segnalazione da parte dei componenti della struttura di eventuali disfunzioni organizzative e/o del sistema dei controlli interni, di eventuali irregolarità nella gestione o di violazioni di norme;
- adeguamento ai requisiti di base in materia di *governance* e organizzazione dell'ICT, gestione del rischio informatico, sicurezza informatica, sistema di gestione dei dati, esternalizzazione di sistemi e servizi;
- obbligo di formalizzare il processo di valutazione delle attività aziendali e di dotarsi di processi e metodologie di valutazione delle attività, anche a fini contabili, affidabili e integrati con il processo di gestione del rischio;
- obbligo di dotarsi di un formale *risk appetite framework*;
- adeguamento alla specifica disciplina inerente ai profili di esternalizzazione di funzioni aziendali.

Infine, si richiede di valutare l'opportunità di **armonizzare i tempi di applicazione di contenuti rivenienti da disposizioni prudenziali in corso di definizione a livello comunitario con quelli di prevista entrata in vigore delle stesse disposizioni,** per non porre gli intermediari nazionali in una posizione di svantaggio competitivo e agevolare il processo di adeguamento all'articolata e complessa evoluzione del quadro di riferimento complessivo.

2. Ruolo, compiti e responsabilità degli organi aziendali

Le disposizioni in consultazione non regolamentano in modo esplicito, diversamente dalle precedenti, ruolo compiti e responsabilità del Direttore Generale nell'ambito del sistema dei controlli interni. In effetti, relativamente a tale figura, queste prevedono esclusivamente che ***"il direttore generale rappresenta il vertice della struttura interna e come tale partecipa alla funzione di gestione"***. Le nuove disposizioni, infatti, prendono logicamente atto dell'evoluzione intervenuta nella disciplina in materia di governo aziendale. Più in generale, il documento fornisce ***"indicazioni minime circa il ruolo di ciascun organo aziendale nell'ambito del sistema dei controlli interni, anche al fine di chiarire i relativi compiti e responsabilità"*** pur non esaurendo tali indicazioni ***"le cautele che possono essere adottate dai competenti organi aziendali nell'ambito della loro autonomia gestionale".***

In tale contesto, la disciplina proposta è improntata a una netta distinzione dei ruoli attribuiti all'Organo con Funzione di Gestione da quelli attribuiti all'Organo con Funzione di Supervisione Strategica. Se ciò facilita la comprensione delle finalità prescrittive della norma in quanto rende ulteriormente esplicita e immediata l'articolazione dei diversi compiti, l'applicazione degli indirizzi così definiti a contesti di tipo "tradizionale" può risultare di complessa declinazione, anche in relazione alla formulazione attuale delle disposizioni statutarie relative agli organi amministrativi.

La necessità di assicurare una corretta interpretazione e applicazione della normativa pone quindi l'esigenza di chiarire, con riguardo a taluni passaggi dispositivi di rilievo, quale sia la corretta declinazione da dare a tali indicazioni.

Le osservazioni che precedono traggono origine anche dalla considerazione che sinora, nel sistema bancario, la Direzione Generale ha svolto un ruolo significativo nell'assicurare la funzionalità del sistema dei controlli interni anche con riferimento all'attività di collegamento tra funzioni di controllo e Organi di Governo. Ciò è particolarmente vero nel Sistema del Credito Cooperativo laddove l'assetto degli Organi aziendali è, come noto, di tipo tradizionale.

Si chiede di confermare la possibilità, con riferimento agli intermediari creditizi che adottino il sistema tradizionale, di incentrare taluni dei compiti definiti in merito alla strutturazione e al funzionamento del sistema dei controlli interni per l'Organo con Funzione di Gestione sulla Direzione Generale, eventualmente dandone una declinazione puntuale e circoscritta. A tale riguardo potrebbe risultare, ad esempio, utile l'introduzione di una prescrizione quale la seguente: "*il direttore generale può essere destinatario di deleghe da parte dell'organo con funzione di supervisione strategica in materia di strutturazione e funzionamento del sistema dei controlli interni*".

Rispetto alla generalità delle tematiche contemplate al punto 3) della Sez. II del documento, la Direzione Generale esercita poteri di proposta all'Organo amministrativo ed è responsabile dell'attuazione delle deliberazioni da questo assunte, ma non è normalmente attributaria di compiti propri, né per legge, né per disposizioni statutarie.

Si rappresenta che i compiti e i poteri della Direzione Generale (non disciplinati dal Codice Civile) sono normalmente attribuiti da parte del Consiglio di Amministrazione con limiti ed ambiti di intervento definiti dallo Statuto sociale e in genere circoscritti alla gestione corrente ed alla esecuzione delle deliberazioni assunte dall'organo amministrativo e, in alcuni casi, estesi alla facoltà di proposta.

Si evidenzia, più in generale, come **diversi riferimenti delle nuove disposizioni** appaiano **innovativi rispetto alle attribuzioni attualmente disciplinate nello statuto tipo delle BCC-CR**.

Si rammenta che, successivamente alle Disposizioni di Vigilanza sul governo societario del 2008, lo statuto tipo delle BCC-CR è stato modificato attribuendo competenza esclusiva in tema di nomina dei responsabili delle funzioni di controllo interno al Consiglio di Amministrazione, organo in tale momento operante nella funzione di supervisione strategica (art. 35). Le disposizioni in consultazione modificano nettamente tale competenza
Il potere di nominare e revocare i responsabili delle funzioni aziendali di controllo, viene infatti attribuito "***all'organo con funzione di gestione, d'accordo con l'organo con funzione di***

supervisione strategica, sentito l'organo con funzione di controllo" (Sez. III, par. 1). Tale disposizione appare coerente con quanto stabilito dal regolamento Congiunto Banca d'Italia/Consob del 2007, che all'art. 12, comma 2, lett. b), prevede che per assicurare la correttezza e l'indipendenza delle funzioni aziendali di controllo è necessario, tra l'altro, che "***i responsabili [...] siano nominati dall'organo con funzione di gestione, d'accordo con l'organo con funzione di supervisione strategica, sentito l'organo con funzione di controllo***". Pur comprendendo l'esigenza di uniformare le disposizioni in materia di controlli, in particolare quelle che afferiscono all'istituzione di funzioni aziendali di controllo, si rappresenta che tale attribuzione si pone in discontinuità con quanto stabilito dalle Disposizioni di vigilanza del 10 luglio 2007 sulla funzione di conformità (p. 7) e di quelle sul governo societario del 4 marzo 2008 (p. 6); tali ultime disposizioni trovano, peraltro, puntuale riscontro nello Statuto tipo delle BCC-CR che, come cennato, attribuisce tale non delegabile competenza al Consiglio di Amministrazione, sentito il Collegio Sindacale.

Un'altra attribuzione che sembra innovare una delle competenze disciplinate dallo statuto tipo delle BCC-CR riguarda l'attribuzione all'organo di controllo dei compiti dell'organismo di vigilanza ai sensi della 231/2001, organismo la cui costituzione, nonché composizione e disciplina, sono stati attribuiti come competenza indelegabile al Consiglio di Amministrazione nell'ultima revisione dello Statuto tipo delle BCC-CR avvenuta nel 2011. Peraltro, il provvedimento in parola, al paragrafo 4 della Sezione II, in cui vengono descritti i compiti e le responsabilità dell'organo con funzione di controllo, sembra rendere obbligatorio per le banche l'adozione del modello organizzativo previsto dalla legge n. 231/2001 sulla responsabilità amministrativa degli enti. Diversamente, al paragrafo 5 della medesima sezione, dove si afferma che il corretto funzionamento del sistema dei controlli interni si basa sulla proficua interazione tra tutte le funzioni e organi (interni e societari) con compiti di controllo, si ricorda anche l'organismo di vigilanza "eventualmente" istituito ai sensi della legge n. 231/2001. In tale contesto, l'adozione di detto modello organizzativo sembra essere facoltativa. Tale ultima lettura appare, peraltro, coerente con il quadro ordinamentale introdotto dalle recenti norme in tema di liberalizzazioni e semplificazioni. Pertanto, alla luce di quanto sopra riportato, si propone di riformulare il periodo del paragrafo 4, relativo all'attribuzione all'organo di controllo dei compiti dell'organismo di vigilanza, nel seguente modo: "*L'organo con funzioni di controllo svolge altresì le funzioni dell'organismo di vigilanza – **eventualmente** previsto ai sensi della legge n. 231/2001, in materia di responsabilità amministrativa degli enti – che vigila sul funzionamento e l'osservanza dei modelli di organizzazione e di gestione di cui si dota la banca per prevenire i reati rilevanti ai fini della medesima legge*".

Con riferimento agli indirizzi in materia di governo e organizzazione dell'ICT di cui al Capitolo 8 del Titolo 5, Sezione II, si segnala:

- relativamente al **Paragrafo** 1**; Comma** 1; **Alinea** 3 ***"Compiti dell'Organo con funzione di supervisione strategica",*** l'opportunità di precisare l'asserzione secondo cui tale Organo ***"... promuove strumenti e modalità organizzative per lo sviluppo, la condivisione e l'aggiornamento di conoscenze in materia di ICT all'interno***

dell'azienda …". Il rilievo oltre che il ruolo dell'Organo in questione sembrano consigliare l'eliminazione del riferimento a *"… strumenti e modalità organizzative.."* riformulando l'asserzione in *"… promuove lo sviluppo, la condivisione e l'aggiornamento di conoscenze in materia di ICT all'interno dell'azienda …".* Peraltro, il circoscrivere l'ambito di tale prescrizione alla *"materia ICT"* sembra avere un carattere contingente.

- relativamente al **Paragrafo** 2**; Comma** 1; **Alinea** 2 *"Compiti dell'Organo con funzione di gestione",* l'asserzione secondo cui l'Organo di gestione *"… disegna e segue l'implementazione dei processi di gestione dell'ICT …"* appare meritevole di una riformulazione, da un lato finalizzata ad evitare che una impropria interpretazione del termine *".. disegna …"* possa far attribuire all'Organo compiti esecutivi, dall'altro lato finalizzata a meglio distinguere il ruolo dell'organo di gestione dal ruolo del cosiddetto "Direttore dei sistemi informativi" (cfr. **Paragrafo** 3; **Comma** 1; **Alinea** 1).
- relativamente al **Paragrafo** 2**; Comma** 3 *"Compiti dell'Organo con funzione di gestione",* l'asserzione secondo cui l'Organo con funzione di gestione *"… indipendentemente dall'articolazione organizzativa dell'intermediario e dalle strategie di sourcing adottata per l'ICT, … deve essere dotato di competenze tecnico – manageriali coerenti con le responsabilità ed i compiti menzionati…."* appare di problematica applicazione ai contesti di tipo tradizionale in generale, delle piccole banche in particolare;
- relativamente al **Paragrafo** 1**; Comma** 3 *"Compiti dell'Organo con funzione di gestione", l'asserzione secondo cui "…approva gli standard di data governance, le procedure di gestione dei cambiamenti e degli incidenti e, di norma con cadenza annuale, il piano operativo delle iniziative informatiche, verificandone la coerenza con le esigenze informative e di automazione delle linee di business nonché con le strategie aziendali.."* appare problematica, ove non opportunamente declinata , qualora i sistemi ed i servizi ICT siano stati esternalizzati e conseguentemente *l'outsourcer* debba fornire il proprio contributo per consentire ai clienti di assolvere alle proprie funzioni, tra le quali la redazione dei documenti previsti nell' allegato A: relativamente al piano operativo delle iniziative informatiche si prospetta, infatti, una criticità associata alla trasparenza dell'informativa da fornire. Nel piano delle iniziative informatiche dell'*outsourcer* potrebbero essere previste anche evoluzioni miranti ad acquisire un vantaggio competitivo nei confronti di altri soggetti concorrenti; in tale evenienza si presenterebbe una rilevante contrapposizione di interessi tra la necessità di mantenere un riserbo rigoroso sugli sviluppi in corso e quella di fornire ampia visibilità sul piano.

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**.

3. Esternalizzazione delle funzioni aziendali

Tra le novità di maggior rilievo per la Categoria, rientra certamente la definizione di una specifica disciplina inerente ai profili di esternalizzazione di funzioni aziendali[1].

A tale riguardo, si evidenzia come **le previsioni contenute nel documento di consultazione sembrano di fatto assimilare l'esternalizzazione da/a aziende facenti parti del medesimo network o, nell'ambito di un gruppo bancario, alla capogruppo, all'esternalizzazione verso soggetti terzi, assoggettando,** pertanto, i vari soggetti coinvolti **ai medesimi obblighi**. Con ciò **non sembrano tenere conto dell'intrinseco interesse della capogruppo ad assicurare la fornitura di servizi adeguati e in linea con i principi esposti nel documento e della circostanza che nel *network* le strutture, associative o imprenditoriali, che forniscono attività alle BCC-CR, sono costituite e operano nella logica esclusiva di servizio alle aderenti**.

Pur non potendo non condividere la necessità di rafforzare i presidi a fronte dei rischi inerenti alle attività e funzioni esternalizzate (data anche la rilevanza che l'*outsourcing* assume nel sistema del credito cooperativo anche in termini di declinazione operativa della proporzionalità ai fini dell'adeguamento a un quadro regolamentare sempre più articolato e complesso) la formulazione sulla cui base ***"le banche che adottano scelte di outsourcing devono presidiare i rischi derivanti dalle scelte effettuate, mantenendo la capacità di controllo e la responsabilità sulle attività esternalizzate nonché le competenze tecniche e gestionali essenziali per re-internalizzare in caso di necessità il loro svolgimento"*** potrebbe determinare oneri impropri in rapporto ai benefici effettivamente

[1] Le disposizioni attribuiscono agli organi aziendali la responsabilità di assumere e attuare una policy interna che regolamenti l'assunzione delle decisioni in materia di outsourcing nell'ambito della quale devono essere valutati, perlomeno, i seguenti aspetti:

- preventiva analisi costi/benefici. La valutazione dei costi e benefici dei rischi alla base della soluzione di outsourcing adottata devono essere chiaramente valutati e documentati e l'analisi deve essere periodicamente aggiornata;
- individuazione delle procedure da seguire nell'esternalizzazione delle attività essenziali;
- analisi dei rischi derivanti dalla concentrazione di attività presso un unico fornitore e dall'esternalizzazione di più attività ad uno stesso fornitore che possono comportare l'insorgere di conflitti di interesse;
- predisposizione di procedure che assicurino la capacità di supervisionare le attività date in outsourcing, al fine di intraprendere tempestivamente eventuali azioni correttive (struttura di governance con ruoli e responsabilità chiaramente definiti; ciò implica, ad esempio, l'individuazione di un referente interno responsabile del monitoraggio e della gestione del contratto di outsourcing);
- definizione di adeguate misure per assicurare la compliance normativa;
- definizione dei contingency plan e delle strategie da adottare ai fini della chiusura anticipata dei contratti di esternalizzazione;
- disciplina delle norme di comportamento nelle varie fasi del processo di outsourcing (decisione dell'esternalizzazione, attività di due diligence sul fornitore del servizio, definizione del contratto di outsourcing, implementazione, monitoraggio e gestione dello stesso..);
- formalizzazione di un contratto che definisca in modo chiaro tutti gli aspetti dell'accordo (chiara definizione di compiti e responsabilità, anche in tema di compliance, adeguata remunerazione dei servizi prestati;…);
- obbligo di produrre entro il 30 aprile di ogni anno una relazione, redatta dalla funzione di revisione interna o, qualora questa sia esternalizzata, dal referente interno aziendale, relativa ai controlli svolti sulle funzioni operative importanti esternalizzate, alle carenze eventualmente riscontrare e alle conseguenti azioni correttive adottate

prodotti. Laddove non opportunamente declinata, tale previsione sembrerebbe imporre anche alle BCC-CR e alle aziende rientranti nel perimetro di un gruppo che decidono di esternalizzare o accentrare, in un'ottica di efficienza ed efficacia della soluzione adottata, determinate attività o funzioni, rispettivamente, all'interno del network o alla capogruppo, il mantenimento di presidi competenziali tali da poter re-internalizzare in ogni momento le attività stesse, con ciò vanificando i presupposti stessi della scelta operata.

Con riguardo all'esternalizzazione di funzioni operative importanti, le disposizioni richiedono che ***"siano soddisfatte le seguenti condizioni:***

- ***.....a) conserva la competenza richiesta per controllare efficacemente le funzioni esternalizzate e per gestire i rischi connessi con l'esternalizzazione, inclusi quelli derivanti da potenziali conflitti di interesse dell'outsourcer, in tale ambito individua, all'interno della propria organizzazione, un responsabile del controllo delle singole funzioni esternalizzate dotato di adeguati requisiti di professionalità ("referente per le attività esternalizzate")."***

Nelle realtà di dimensioni contenute - come le BCC-CR - la scelta di esternalizzare attività, processi o funzioni è generalmente dettata dalla necessità di mantenere strutture snelle e al tempo stesso in grado di far fronte alla crescente complessità operativa e regolamentare. Per le BCC-CR, pertanto, l'obbligo di mantenere le competenze tecniche gestionali essenziali per re-internalizzare, in caso di necessità, lo svolgimento delle attività esternalizzate risulterebbe antieconomico oltre che di difficile attuazione. Ma anche la necessità di individuare un ruolo responsabile dotato delle necessarie competenze e requisiti di professionalità per esperire controlli di merito potrebbe determinarsi impropriamente oneroso, con il rischio di ridursi a un mero adempimento formale. Peraltro, va tenuto presente che nell'esternalizzazione le BCC-CR ricorrono nella generalità dei casi a società/enti appartenenti al Sistema del Credito Cooperativo che offrono soluzioni coerenti con le peculiari caratteristiche delle BCC-CR stesse e maggiori garanzie rispetto a soggetti terzi presenti sul mercato.

Più in generale, si ritiene che sia **le valutazioni di opportunità** - **all'atto della scelta e periodiche** - sia **la definizione degli adeguati presidi in ordine al corretto svolgimento delle attività conferite**, ferma la responsabilità aziendale sulle stesse, **debbano trovare in un network e in gruppo bancario risposta a un livello diverso da quello della singola azienda/controllata**.

Nel Sistema del Credito Cooperativo italiano, l'attuale modello di *governance* delle strutture di secondo livello, associative e imprenditoriali, riflette la *governance* delle BCC-CR. Tale modello ha espresso nel tempo la propria efficacia con riguardo alla capacità di un sistema composto da entità giuridicamente autonome di operare nel perseguimento di obiettivi comuni e condivisi. Si ritiene che tale peculiare meccanismo di *governance*, ulteriormente rafforzato (in particolare, proprio con riguardo al governo dei profili di rischio delle aderenti) dalla costituzione del Fondo di Garanzia Istituzionale, possa e debba costituire la base sulla quale costruire, in coerenza e sinergia con le attività già in corso per la razionalizzazione

della filiera associativa, gli interventi necessari per rafforzare il presidio dei rischi sottesi alle funzioni e attività esternalizzate e conseguire il progressivo innalzamento del livello di qualità delle stesse nell'interesse di tutte le entità aderenti.

Ne deriva la consapevolezza, per gli Enti di Categoria, della necessità di attivare iniziative coordinate a livello centrale volte al presidio delle attività esternalizzate tramite la definizione delle linee guida da seguire negli accordi di esternalizzazione e di *policy* in materia di esternalizzazione delle attività aventi rilevanza strategica e gestione dei relativi rischi per assicurare il rispetto della normativa e degli standard di riferimento.

Alla luce di tali definizione si potrà:

- procedere gradualmente alla verifica della loro corretta applicazione al fine di assicurare un adeguato grado di aggiornamento e di *compliance* normativa degli accordi attualmente esistenti fra le BCC-CR e i fornitori sui quali le attività sono state esternalizzate;
- formalizzare e/o aggiornare le modalità di erogazione dei servizi e gli SLA (*service level agreement*) per la valutazione del livello di servizio erogato dal fornitore nonché gli obblighi di *compliance* che il fornitore deve osservare;
- **definire un processo di monitoraggio del livello di servizio erogato** e individuare **adeguati strumenti** per la valutazione della *performance* quali, ad esempio, **report sui servizi svolti, autocertificazione, *review* indipendenti da parte dei revisori interni e/o esterni del fornitore o della BCC-CR**;
- assicurare modalità, coordinate centralmente, efficaci ed efficienti per verificare, ad esempio con riguardo ai servizi ICT, il rispetto delle *best practices* e degli standard internazionali di riferimento;
- con particolare riferimento all'esternalizzazione dei servizi finanziari (in un contesto caratterizzato dal generalizzato ricorso *all'outsourcing* dei servizi di valutazione e pricing degli strumenti finanziari, esecuzione dei test di efficacia ai fini dell'Hedge Accounting, etc…) e di back office, ai relativi presidi di controllo, alla definizione di contratti relativi e delle SLA di servizio:
    - verificare l'esistenza di standard contrattuali e SLA in cui siano identificati gli obiettivi di *performance* quali-quantitativi tali da consentire la valutazione dell'adeguatezza dei servizi prestati;
    - individuare adeguati strumenti e modalità per la valutazione della performance del servizio di *outsourcing,* assegnando i relativi ruoli responsabili;
    - definire gli obblighi di *compliance* che il fornitore deve osservare, con particolare riferimento alla validazione dei modelli valutativi, alle attività di *backtesting*, alla verifica sistematica dei prezzi e dei presidi di controllo, alle attività di documentazione dei controlli eseguiti, alla risoluzione o mitigazione dei conflitti di interesse.

Con riguardo al **referente** per le attività esternalizzate si ritiene opportuno operare un distinguo, per le BCC-CR, tra due famiglie di "esternalizzazioni": quelle di "**controllo**" (secondo e terzo livello) e quelle delle "**funzioni operative importanti**".

Con riguardo alle prime, in coerenza con il quadro normativo vigente, è già oggi presente una figura (il responsabile interno della Funzione esternalizzata o con riguardo alla revisione interna, il Referente interno) connotato delle caratteristiche e prerogative necessarie per un adeguato monitoraggio della qualità e rispondenza del servizio prestato dall'*outsourcer*.

Gli obblighi di valutare l'adeguatezza delle Funzioni di Controllo sono, inoltre, incardinate - in seno alla Revisione interna - con periodicità che definisce l'azienda e a prescindere dall'esternalizzazione o meno delle stesse.

Con riguardo alle seconde, si ritiene necessario che le disposizioni prevedano un'adeguata flessibilità organizzativa delle soluzioni applicabili per il controllo delle singole funzioni esternalizzate, **riconoscendo e valorizzando in tale ambito anche le caratteristiche e potenzialità dell'organizzazione a rete del sistema del credito cooperativo.**

Le disposizioni in consultazione prevedono che le banche siano tenute alla tempestiva trasmissione alla Banca d'Italia delle relazioni annuali sulle attività svolte da parte delle funzioni aziendali di controllo. **Qualora tali funzioni siano esternalizzate, la relazione è prodotta dai referenti aziendali delle stesse**.
A tale riguardo, **pur nella consapevolezza della maggiore onerosità che questa produce,** si esprime condivisione **in merito all'attribuzione del compito di redigere tale relazione al referente aziendale.** Si ritiene infatti imprescindibile il coinvolgimento di un ruolo interno all'azienda sia per assicurare l'adeguato *commitment* in merito alle evidenze sottoposte dalla funzione di controllo, sia per integrare le evidenze critiche sottoposte all'Organo di Vigilanza con i necessari riferimenti riguardo alle iniziative che il Consiglio di Amministrazione della banca ha pianificato o avviato per la risoluzione delle criticità eventualmente emerse. Il referente aziendale assume, in altre parole, un ruolo fondamentale nell'agevolare il processo di pianificazione e costante monitoraggio degli interventi di mitigazione dei rischi individuati oltre che nell'assicurare la capacità di dare pienamente conto alla Vigilanza delle azioni intraprese.

Le disposizioni richiedono, inoltre, che entro il 30 aprile di ogni anno le banche trasmettano alla Banca d'Italia ***"una relazione, redatta dalla funzione di revisione interna - o, se esternalizzata, dal referente aziendale - con le considerazioni dell'organo con funzione di controllo e approvata dall'organo con funzione di supervisione strategica, relativa ai controlli svolti sulle funzioni operative importanti esternalizzate, alle carenze eventualmente riscontrate e alle conseguenti azioni correttive adottate."***

La previsione normativa relativa all'invio di una relazione, redatta dalla funzione di revisione interna – **o, se esternalizzata dal referente aziendale** - comporta una **significativa**

modifica rispetto alle attuali e note modalità di erogazione del servizio di *Internal Auditing* in capo alle strutture associative.

Le attività di controllo sulle funzioni operative importanti esternalizzate potrebbero essere svolte per conto delle BCC-CR dalla Funzione di Revisione interna, nella generalità dei casi esternalizzata alla Federazione di competenza, evitando così oneri eccessivi per le banche ed ostacoli all'operatività degli *outsourcer* che si determinerebbero laddove ogni BCC-CR procedesse in autonomia ai previsti controlli (con modalità analoghe, ad esempio, a quanto già attualmente in essere riguardo all'*Information system audit*).
La relazione verrebbe inviata al **referente aziendale** il quale provvederebbe ad integrarla con le **considerazioni** del **Collegio Sindacale** e, dopo la **valutazione e approvazione del Consiglio di Amministrazione**, alla trasmissione alla Banca d'Italia.

Le modalità per la realizzazione delle attività di *audit* che poi confluiranno nella Relazione Annuale possono essere racchiuse in due modelli: uno "**diretto**" ed uno "**indiretto**".

Nel primo, l'*Internal Auditing* opera presso *l'outsourcer* e presso la Banca. Il Servizio, dopo aver definito uno specifico **processo per il controllo delle funzioni operative importanti esternalizzate,** svolgerebbe tale attività con modalità analoghe a quelle ormai consolidate nell'ambito dell'I*nformation System Auditing*. Ciò consentirebbe la realizzazione di importanti economie di scala.

L'applicazione del modello "**indiretto**" prevede, invece, lo svolgimento delle attività di controllo nell'ambito dei processi già previsti nell'ambito del contratto di *Internal Audit*. L'applicazione di tale metodologia verrebbe comunque resa onerosa, inefficace e/o ridondante dalle seguenti ragioni:

- cadenza annuale di invio della relazione alla Banca d'Italia;
- eccessiva frammentazione dei controlli relativi al singolo processo;
- assenza di una visione di insieme sulle attività esternalizzate;
- ripetizione delle medesime attività di controllo presso una pluralità di BCC-CR.

Ambedue le opzioni comporterebbero la necessità di potenziare le strutture di Internal Audit attuali.

ESTERNALIZZAZIONE NEI GRUPPI BANCARI

Con particolare riguardo ai profili di outsourcing interni a **un Gruppo Bancario,** le disposizioni in consultazione, al fine di assicurare l'effettività e l'integrazione dei controlli, richiedono che l'esternalizzazione delle funzioni aziendali di controllo presso la Capogruppo o le altre componenti del Gruppo sia attuata nel rispetto di principi e presupposti ulteriori rispetto a quelli previsti alla sezione IV.

Si evidenzia innanzitutto la necessità di effettuare un opportuno distinguo tra **accentramento** ed **esternalizzazione,** circostanze assai eterogenee che devono essere valorizzate anche in ottemperanza al principio di economicità.

Nel richiamare nuovamente le considerazioni già anticipate riguardo all'intrinseco interesse della Capogruppo a fornire servizi adeguati e in linea con i principi esposti nella Sezione 4 (livelli di servizio, competenza, tempestività nell'informazione, sicurezza, ecc.), a integrazione o maggiore evidenza di quanto già commentato, si riportano nel seguito ulteriori osservazioni, dettagliate per ciascuno dei criteri definiti nel documento di consultazione.

- ***"a) devono essere chiaramente valutati e documentati i costi, i benefici ed i rischi alla base della soluzione adottata; tale analisi deve essere periodicamente aggiornata"***

L'accentramento presso la Capogruppo delle Funzioni di Controllo costituisce una scelta di *governance* che intende contestualmente perseguire *i)* una maggiore efficienza interna *ii)* l'efficacia dell'azione di controllo attraverso la creazione di centri di competenza specialistici *iii)* la costituzione di un presidio unitario dei rischi che fornisca concreta attuazione del principio di responsabilità della Capogruppo, ferme le responsabilità individuali degli Organi Aziendali delle Società Controllate in materia di assunzione, gestione e controllo dei rischi.
Le caratteristiche attuative di tale scelta di *Governance*, anche in termini di attività, responsabilità ed attribuzioni, modalità di espletamento, rappresentazione e diffusione degli esiti, relazione/rapporto con gli Organi Aziendali della Società Controllata, governo operativo della Funzione sono di norma disciplinate nel Regolamento di *Corporate Governance* del Gruppo Bancario. Detto regolamento assolve gli obblighi di disciplina dell'esercizio delle Funzioni di Controllo presso la Capogruppo e le Società Controllate unitamente ai Regolamenti interni aziendali che recepiscono e definiscono compiti, ruoli e responsabilità delle Funzioni di Controllo accentrate presso la Capogruppo.

Si ritiene, in sostanza che l'accentramento delle Funzioni di Controllo non debba essere assimilato ad un concetto di esternalizzazione bensì ad una scelta di *governance* volta ad unificare il presidio dei rischi, con particolare riferimento al secondo e al terzo livello di controllo. L'esercizio della responsabilità da parte degli Organi Aziendali delle Società Controllate risulta assolvibile attraverso una puntuale previsione di obblighi e responsabilità della Funzione di Controllo accentrata verso gli stessi Organi Aziendali delle Società Controllate.

In tale ambito, i profili richiamati dalle disposizioni in consultazione sono nella sostanza intrinsecamente valutati attraverso gli ordinari compiti di monitoraggio sull'efficace ed efficiente funzionamento delle funzioni di controllo esternalizzate alla Capogruppo svolti dai Consigli di Amministrazione delle Controllate e della Capogruppo stessa. Una "formale" verifica in tal senso non aggiungerebbe profili di sostanziale utilità ulteriore stante il già

richiamato interesse della Capogruppo a fornire servizi adeguati anche sotto il profilo del presidio di tutti i rischi.
Le logiche di accentramento, inoltre possono non necessariamente, in funzione del complessivo modello di controllo e sotto la responsabilità della Capogruppo, rispettare alcuni dei criteri citati: in tali casi le valutazioni (anche periodiche) della controllata non dovrebbero assumere rilievo. Si chiede di chiarire, perlomeno, che la valutazione in argomento spetta esclusivamente alla Capogruppo e sia da effettuarsi con riguardo a una valutazione integrata per il gruppo nel suo complesso.

- ***b) 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 ….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)***

La formulazione, che, di fatto, sembra imporre un modello decentrato di controllo non sembra adeguata a rappresentare la realtà di tutti i gruppi bancari.

Si riterrebbe più congruo disciplinare i requisiti (ad esempio, in termini di numero di società controllate/filiali, dimensioni delle medesime e del gruppo nel suo insieme) che fanno propendere per la scelta di un modello accentrato o decentrato. In ogni caso, le indicazioni nel documento di consultazione potrebbero generare potenziali inefficienze nell'interfaccia con le controllate specie nei contesti di Gruppo nei quali l'operatività delle Funzioni di Controllo si realizza in via ordinaria senza referenti interni, potendo contare - in caso di problemi – sull'ordinaria interlocuzione con la Direzione Generale.

Più in generale, la previsione richiamata appare in contrasto con:

- il principio di efficienza alla base della scelta di accentramento, posta l'evidente anti economicità del riferimento specifico al referente interno e al mantenimento delle competenze in una logica di complessivo assetto del Sistema dei Controlli Interni di Gruppo;
- la tipologia di relazione Capogruppo-Controllata e le regole di Governance del Gruppo Bancario con riferimento
- ad eventuali clausole risolutive per impossibilità, incapacità o mancato rispetto dei livelli di servizio
- ad un obbligo di controllo e quindi di relazione degli esiti da parte dalla funzione di revisione interna - o, se esternalizzata, dal referente aziendale – che non sia riconducibile al normale assoggettamento di tutte le funzioni aziendali al controllo

della revisione interna esercitato su base individuale o a livello consolidato secondo le previsioni in materia di "Controlli interni di Gruppo", Sez. 5, paragrafo 2.

Tutto ciò premesso si richiede:

- di sostituire il riferimento alla Sezione 4 con specifiche previsioni / obblighi delle Funzioni accentrate verso gli Organi Aziendali delle Società Controllate;
- di prevedere in tale ambito che l'obbligo per le Società Controllate di individuare, all'interno della propria organizzazione, un responsabile del controllo della singola funzione di Controllo accentrata presso la Capogruppo, sia assolto attraverso l'attribuzione di tale responsabilità alla Direzione Generale della stessa Società Controllata.

- ***c) 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***

La formulazione proposta appare non pienamente condivisibile per i seguenti motivi:

- verrebbero meno le sinergie derivanti dall'effettuazione di attività sia a valere della Capogruppo sia a valere delle Controllate, attuate mediante un'allocazione efficiente dei profili competenziali sottesi ai progetti di accentramento: ciò al solo fine di poter tracciare gli auditors dedicati e la loro adeguatezza quali-quantitativa. Tra l'altro il criterio prevalente di specializzazione delle risorse di auditing è per ambito/processo, impostazione questa ritenuta maggiormente atta a garantire efficacia ed efficienza di quella per singola entità o per Capogruppo *vs* entità controllate;

- eventuali conflitti di interesse sono già gestiti con le procedure adottate ai fini della *quality assurance review* – QAR, in corso di attestazione. Le funzioni certificate hanno ottenuto la QAR avendo dimostrato, fra l'altro, di disporre di idonee procedure atte a garantire giudizi indipendenti.

In estrema sintesi, la soluzione proposta nelle disposizioni i consultazione potrebbe risultare inefficiente e comporterebbe, comunque, oneri cospicui di rinforzo degli organici. Si ritiene utile escludere tali obblighi di separatezza per le funzioni affidate alla Capogruppo e dotate di processi certificati per la gestione dei conflitti di interesse.

"La Capogruppo invia annualmente alla Banca d'Italia una relazione riguardante gli accertamenti effettuati sulle società controllate.

Nel caso di gruppi bancari, inoltre, le rispettive capogruppo coordinano e trasmettono alla Banca d'Italia, per tutte le banche del gruppo, la stessa documentazione richiesta nel caso delle banche non appartenenti a gruppi bancari".
"Le relazioni sulle attività svolte dalle funzioni aziendali di controllo della capogruppo contengono anche gli esiti delle verifiche effettuate, dei risultati emersi, dei punti di debolezza rilevati con riferimento, oltre che alla capogruppo medesima, anche al gruppo bancario nel suo complesso e descrivono gli interventi da adottare per la rimozione delle carenze rilevate".

Si ritiene opportuno prevedere - nel caso di funzioni accentrate di *Internal Audit* - l'invio di un'unica relazione che rappresenti il contenuto delle attività svolte a valere su ciascuna società Controllata nonché sulla Capogruppo, evidenziando, quindi, sia gli aspetti di criticità relativi ad una specifica società sia gli effetti sul gruppo nel suo complesso.

Infine, sempre con riguardo ai profili di *outsourcing* interni al Gruppo, si evidenzia che il ricorso alla formalizzazione di un contratto tra le parti si ritiene utile in una logica di ripartizione dei costi e dunque di definizione dei corrispettivi economici in capo a ciascun componente del Gruppo, ritenendolo invece non necessario nei casi nei quali non sussistano presupposti o esigenze di tale natura.

4. Sistema informativo

Pur mitigato dal richiamo al principio di proporzionalità ***("le concrete misure da adottare possono essere individuate tenendo conto, oltre che degli specifici obiettivi strategici, anche, sulla base del principio di proporzionalità, delle dimensioni dell'intermediario, del tipo e della complessità della sua operatività, dal livello di automazione dei suoi processi e servizi")*** l'indiscutibilmente utile riferimento alle *best practices* quale criterio guida nella impostazione dei sistemi di governo e controllo dei profili ICT ***("… in tale ambito, gli intermediari fanno riferimento agli standard e alle best practices definiti a livello internazionale in materia di governo, controllo e sicurezza dei sistemi informativi …")*** non può non avere riflessi di rilievo sull'organizzazione aziendale e, in alcuni casi, sullo stesso modello di business. Conseguentemente, la piena efficacia di tale adozione, comunque da declinare in funzione del richiamato principio di proporzionalità, non può prescindere dal progressivo conseguimento di successivi "livelli di maturità" organizzativa.
Si ritiene che le disposizioni dovrebbero focalizzarsi su indirizzi strategici (quali quelli contenuti nel **Paragrafo** 1 ***" .. gli intermediari fanno riferimento agli standard e best practices …")*** e su contenuti che si condivide appaiono indispensabili per una consapevole assunzione dei rischi (cfr. Sezione III, approvazione del rischio residuo) senza richiamare espressamente nella normativa componenti anche importanti delle citate *best practices* che dovrebbero trovare sempre una declinazione basata sul generale principio di proporzionalità e di "*capability level*" organizzativo.

Ad ulteriore evidenza, l'estrapolazione dal contesto di alcune parti delle *best practices* indicate al **Titolo** V, **Capitolo** 8, **Paragrafo** 2 (COBIT, ITIL, ISO/IEC 27002:2005) potrebbe ingenerare dubbi interpretativi e difformità di applicazione che ne potrebbero limitare l'efficacia: nella definizione pertanto sarebbe preferibile fare riferimento al complessivo sistema di standard e delegarne l'applicazione secondo i criteri summenzionati.

Il cambiamento degli standard nel corso degli ultimi anni (il passaggio dai British Standard agli ISO standard) potrebbe inoltre rendere non attuale e non coerente con lo standard in vigore le parti estrapolate ed inserite nella normativa rendendola, di fatto, non completamente comparabile.

Entrando nel merito delle specifiche previsioni, di seguito si riportano in dettaglio i profili critici rilevati.

TITOLO V; CAPITOLO 8; SEZ. II; PARAGRAFO 3; COM. 1; ALI. 4 - "ORGANIZZAZIONE DELLA FUNZIONE IT"

Con riferimento alle attività di analisi del rischio informatico, le disposizioni precisano che ***"…. fermo restando quanto previsto nel Capitolo 7, Sezione III per le funzioni aziendali di controllo di secondo e terzo livello, l'attribuzione formale dei compiti di analisi del rischio informatico e di emanazione e verifica della policy di sicurezza ICT, da svolgere, nelle realtà più complesse, con personale con adeguate caratteristiche professionali e di specializzazione nella materia, va garantita l'indipendenza di giudizio rispetto alle funzioni operative …".***
La precisazione di cui all'ultimo capoverso, secondo cui va garantita l'indipendenza di giudizio della funzione preposta all'analisi dei rischi, potrebbe essere interpretata in modo estensivo giungendo sino a richiedere una separazione organizzativo-strutturale simile a quella richiesta per le funzioni di controllo di 2° e 3° livello. Se ciò può risultare in linea di principio utile perché rafforza la "*segregation of duty*" non sembra però, né indispensabile (non trattandosi di una entità di controllo di 2° o 3° livello), né funzionale alle finalità dell'efficace esercizio della funzione richiamata.
Nel contempo, si sottolinea l'opportunità di prescrizioni finalizzate a garantire un tempestivo, completo e corretto flusso di informazioni dalle funzioni operative alla funzione sicurezza e da questa alla funzione rischi operativi.
Ferme restando quindi le finalità di ***"garantire l'indipendenza di giudizio" e di "utilizzare per il compito personale con adeguate caratteristiche professionali",*** si riterrebbe utile chiarire che tale ***"… indipendenza di giudizio …"*** non postula necessariamente l'adozione di misure di separatezza organizzativo-strutturale quali quelle richieste per le funzioni di controllo di 2° e 3° livello, ma solo la previsione di linee di riporto informativo che ne rafforzino l'indipendenza e l'efficacia.

TITOLO V; CAPITOLO 8; SEZ. III - "LA GESTIONE DEL RISCHIO INFORMATICO"

Al **Comma** 2 si afferma che ***"… il processo di analisi deve essere svolto dall'utente responsabile con la partecipazione del personale tecnico, secondo una metodologia definita dall'organo con funzione di gestione …".***
A riguardo, si osserva che l'assegnazione della primaria responsabilità di svolgimento dell'analisi all'utente, se da un lato ne garantisce la piena e proattiva partecipazione, dall'altro lato può portare a un'incompleta identificazione/valutazione del rischio sotteso.
Si riterrebbe quindi utile modificare il passo in questione o attribuendo la responsabilità di svolgimento dell'analisi alla funzione "*sicurezza*" con previsione di opportune fasi di condivisione con l'utente o riformulando l'attuale prescrizione in "*… il processo di analisi deve essere svolto sotto la responsabilità dell'utente responsabile …*".
Al **Paragrafo** 2, **Comma** 2, Alinea 2 si afferma che ***"… in ogni caso deve essere determinato il rischio residuo da sottoporre ad accettazione formale dell'utente responsabile …".*** Sul punto potrebbe risultare opportuno esplicitare che, qualora il livello di rischio residuo eccedesse i limiti previsti per l'accettabilità da parte dell'utente responsabile, le misure di trattamento del rischio siano sottoposte all'attenzione dell'organo con funzioni di gestione.

TITOLO V; CAPITOLO 8; SEZ. IV -"IL SISTEMA DI GESTIONE DELLA SICUREZZA INFORMATICA"

Al **Paragrafo** 2, **Comma** 1, **Alinea** 5, si afferma che ***"…la separazione degli ambienti di sviluppo, collaudo e produzione, con adeguata formalizzazione del passaggio di moduli software dal primo, al secondo, al terzo (paragrafo 3), al fine di evitare l'accesso a dati riservati e sistemi critici da parte del personale addetto allo sviluppo e di esercitare un più stretto controllo degli accessi e delle modifiche nell'ambiente di produzione …".***
Premessa la piena condivisione dell'irrinunciabile principio di separatezza fra ambienti di sviluppo e produzione, si segnala l'opportunità di meglio circostanziarlo al fine di regolamentare situazioni in cui una parte ben identificata del personale di sviluppo svolga anche compiti di assistenza agli utenti e, nello svolgimento di tale attività, possa avere accesso all'ambiente di produzione.
Nel rilevare che quanto previsto dal **Paragrafo** 2, ultimo alinea punto elenco per la registrazione e conservazione delle tracce elettroniche trova corrispondenza con quanto definito dal Garante per la Protezione dei Dati Personali nel suo Provvedimento del 12 maggio 2011 in materia di circolazione delle informazioni bancarie e tracciamento delle operazioni bancarie (come richiamato nella nota 16), si evidenzia che le regole disciplinate divergono per tempi di conservazione delle tracce elettroniche (cinque anni anziché due anni come previsto dal Provvedimento del Garante): al fine di garantire la coerenza con il quadro normativo di cui sopra sarebbe opportuno armonizzare il periodo previsto nonché far partire tale obbligo almeno dal periodo previsto dal Garante per l'avvio della fase di tracciatura (dicembre 2013).

Al **Paragrafo** 3, **Comma** 1 si afferma che ***"… la procedura di gestione dei cambiamenti – formalmente definita - è tesa a garantire un efficace controllo su modifiche,***

sostituzioni o adeguamenti tecnologici di sistemi e procedure nell'ambiente di produzione. Il processo deve svolgersi sotto la responsabilità di una figura o struttura aziendale con elevato grado di indipendenza rispetto alla funzione di sviluppo …".
Sul punto si segnala l'opportunità di chiarire che per funzione di sviluppo si intende far riferimento sia alla funzione di sviluppo applicativo, sia di sviluppo della infrastruttura.

TITOLO V; CAPITOLO 8; SEZ. V -"IL SISTEMA DI GESTIONE DEI DATI"

Si premette la piena condivisione e l'apprezzamento per l'inserimento nella regolamentazione di specifiche prescrizioni in tema *"di gestione dei dati"* sul quale, come riportato nel passo introduttivo, si fonda l'efficacia del sistema di governo dell'azienda.
Più in dettaglio, circa *i "requisiti che il sistema deve soddisfare"* (cfr. **Comma** 2) si riterrebbe opportuno:

- precisare l'articolazione di ruoli e responsabilità richiesta al 3° **Alinea** secondo cui *"…è definito uno standard aziendale di data governance, che individua ruoli e responsabilità delle funzioni coinvolte nel trattamento dell'informazione …".* La prevalente "forma elettronica" dei dati può, infatti, far ritenere il tema del trattamento e, in particolare, del controllo della qualità dei dati di mero interesse della funzione informatica condizionando in modo rilevante l'efficacia del sistema di "data governance". Si riterrebbe quindi opportuno, in sintonia con altri passi della norma (cfr. Sez. III "gestione del rischio informatico", **Comma** 2, ruolo dell'utente responsabile) rafforzare la prescrizione completandola con "… L'articolazione dei ruoli, ferma restando l'autonomia dei soggetti vigilati nella scelta delle forme organizzative a loro più adatte, deve riservare all'utente responsabile i compiti di governo delle regole di trattamento e di controllo sulla relativa osservanza …"
- chiarire il 4° **Alinea** secondo cui *"… l'utilizzo di procedure settoriali (contabilità, segnalazioni, antiriciclaggio, ecc.) non deve compromettere la qualità e la coerenza complessiva dei dati aziendali; a livello consolidato, va garantita l'integrazione tra le informazioni provenienti da tutte le componenti del gruppo….".* Si ritiene, infatti, che il tema che si intende sollevare non sia quello dell'utilizzo di procedure settoriali ma quello della necessità di prevedere processi di alimentazione/controllo dei dati scambiati al fine di garantire *"… la qualità e la coerenza complessiva dei dati aziendali …"*
- chiarire la finalità del 6° Alinea che - affermando che *"i dati devono essere conservati con una granularità adeguata a consentire le diverse analisi ed aggregazioni richieste dalle procedure di sfruttamento"* - potrebbe, ad una prima lettura, sembrare scontato.

TITOLO V; CAPITOLO 8; SEZ. VI -"ESTERNALIZZAZIONE DI SISTEMI E SERVIZI ICT"

Il Paragrafo 2, Comma 3 elenca gli aspetti che debbono essere disciplinati *"… nei contratti con fornitori di sistemi e servizi ICT …".*

Al secondo e terzo Alinea viene evidenziata la necessità di prevedere una "…***… periodica produzione e messa a disposizione dell'intermediario delle opportune copie di backup di dati (database, transazioni, log applicativi e di sistema) ……..;***
……..l'obbligo per l'outsourcer, una volta concluso il rapporto contrattuale, di eliminare, - facendo uso di opportuni strumenti e capacità tecniche, debitamente documentati – qualsiasi copia o stralcio di dati riservati di proprietà dell'intermediario presente su propri sistemi o supporti, in modo da escludere la possibilità tecnica di accessi successivi a dati dell'intermediario da parte del proprio personale o di terzi….".
Sul punto segnala l'opportunità, al fine di rafforzare la sicurezza dei sistemi del committente, di sostituire il termine ***"copie di back-up dei dati"*** con "*copie di backup del proprio patrimonio informatico*".
I fornitori di sistemi e servizi ICT di Categoria (multiutenti) producono periodiche copie di backup con frequenza diversificata in base alle esigenze applicative (giornaliera, mensile, trimestrale, semestrale, annuale,…); tali copie, anche in funzione del contenuto e delle normative vigenti, ad esempio sulla conservazione della documentazione contabile, vengono archiviate con un periodo di ritenzione che può raggiungere i dieci anni.
Inoltre vengono prodotte copie contestualmente ad attività di fusione tra banche, acquisizione o cessione clienti e per altre finalità, ad esempio connesse alla gestione sistemistica, che si sostanziano in una copia "fisica" dei dati presenti sui supporti di origine.
Relativamente al primo dei due aspetti segnalati si evidenzia la necessità di confermare cosa si intenda per "***messa a disposizione"*** evidenziando a riguardo l'assoluta impraticabilità della consegna delle copie di *backup* qualora sia inclusa tra gli adempimenti.

Per quanto concerne il secondo aspetto si ritiene che nella generalità dei casi le attuali procedure operative di distruzione dei dati siano già conformi ad eccezione di quelle relative ai dati contenuti nei supporti di backup.

Tali supporti, infatti, sono numerosissimi ed ognuno di essi contiene dati di più banche.

Oltre all'onerosità di un'operazione di distruzione selettiva di parte del contenuto su backup, l'operazione si sostanzierebbe in un'alterazione della copia stessa che non potrebbe più definirsi come l'immagine di quanto esistente nei sistemi di produzione alla data della copia originaria.

Al **Paragrafo** 3 viene introdotta la tematica del "*cloud computing*" la cui definizione risulta, nel suo utilizzo corrente, estremamente generica e comprendente differenti accezioni di servizi e architetture.
La descrizione fornita nelle norme ***("fruizione delle risorse informatiche nella forma di servizi accessibili via rete e configurabili in modo flessibile")*** rappresenta senza alcun dubbio un passo ulteriore nel circoscrivere la particolare tematica e, tuttavia, risulta ancora non sufficientemente selettiva, potendo ricomprendere anche servizi già forniti nel passato, ma che difficilmente si associerebbero oggi al termine "*cloud computing*", come ad es.

l'utilizzo di sistemi informativi di base sviluppati e forniti da centri servizi specializzati su reti non pubbliche.
Risulterebbe quindi utile introdurre una definizione di "*cloud computing*" che caratterizzi meglio, almeno per le finalità della normativa in consultazione, le condizioni costitutive del *cloud* da assoggettare alle prescrizioni, facendo ad esempio riferimento a:
specifiche tecnologie e architetture ricadenti nella definizione (ad es. l'utilizzo di internet combinato ad una allocazione dinamica – e non programmabile - delle risorse decentrata su diversi centri di elaborazione);
ambito dei servizi a tal fine interessati dal Provvedimento (ad es. servizi finalizzati all'erogazione ed alla gestione di servizi di pagamento, con esclusione di servizi di community verso la clientela (forum, blog, ecc.).

TITOLO V; CAPITOLO 8; ALLEGATO B -"MISURE IN MATERIA DI SERVIZI TELEMATICI PER LA CLIENTELA"

La tematica delle misure in materia di servizi telematici per la clientela risulta già trattata nel Provvedimento di Attuazione del Titolo II del Decreto legislativo n. 11 del 27 gennaio 2010 (PSD) (specificatamente nell'Allegato "*Tipologie di strumenti di più elevata qualità sotto il profilo della sicurezza*") e nelle "*Recommendations for the Security of Internet Payments*" (ECB).
In particolare, alcune delle misure qui richieste, sono individuate dal Provvedimento di attuazione della PSD come "*Requisiti degli strumenti "a maggior sicurezza"*", lasciando ai responsabili dei sistemi il diritto/dovere di implementare soluzioni in base a valutazioni di rischio.
Al fine di facilitare l'implementazione delle misure richieste, risulterebbe utile procedere ad una omogeneizzazione organica dei requisiti o, in questa sede, limitarsi ad un richiamo alle normative esistenti (scelta adottata, ad esempio, nel Provvedimento di attuazione PSD: ***"i prestatori di servizi di pagamento si attengono ai requisiti di sicurezza definiti nell'ambito dell'Eurosistema con riferimento agli strumenti di pagamento offerti alla clientela finale").***
Al **Paragrafo** 1, si afferma che ***"… al fine di attenuare i rischi di frodi e abusi commessi attraverso falsi siti web che replicano l'apparenza di siti di intermediari, devono essere resi disponibili ai clienti appropriati strumenti per riconoscere i siti web utilizzati per l'erogazione di servizi telematici e per verificarne l'autenticità (ad es. nomi di dominio che rispecchiano la denominazione dell'intermediario, certificati digitali emessi da una riconosciuta autorità di certificazione a nome dell'intermediario) …".***

Pur condividendo l'importanza di fornire metodi adeguati per il riconoscimento dei siti internet, i requisiti tecnici richiesti potrebbero non corrispondere alla realtà operativa di diversi intermediari. Si propone quindi eliminare l'elenco tra parentesi: "***(ad es. nomi di dominio che rispecchiano la denominazione dell'intermediario, certificati digitali emessi da una riconosciuta autorità di certificazione a nome dell'intermediario)***".

Infatti, in tema di *home-banking*, sia i nomi di dominio che i relativi certificati di autenticazione, in diversi casi sono associati a nomi o marchi relativi al servizio stesso o al suo fornitore. Ciò risulta maggiormente vero per intermediari di contenute dimensioni che utilizzano, per tali tipologie di servizi, specifici fornitori.

L'utilizzo di specifici fornitori di servizio è poi pratica diffusa in tema di autenticazione delle transazioni internet legate alle Carte di pagamento (fornitori del servizio cosiddetto 3D-Secure).

In entrambi i casi, l'utilizzo di fornitori specializzati limita gli impatti economici sul singolo intermediario e può favorire l'implementazione di sistemi complessivamente più sicuri.

Sempre al Paragrafo 1, si afferma che ***"…Il canale di comunicazione telematica tra intermediario e cliente deve essere cifrato – mediante robuste soluzioni tecnologiche – senza soluzione di continuità (modalità end-to-end), ogni qualvolta siano scambiati dati personali o comunque riservati, ovvero si acceda a funzioni dispositive …"***

L'utilizzo del semplice termine tecnico "*end-to-end*" in relazione al canale di cifratura dei dati tra intermediario e cliente, non tiene conto della reale architettura dei sistemi internet, in cui il canale di cifratura è continuo tra il dispositivo del cliente ed il sito internet stesso, ma non oltre.
Risulta tecnicamente più completa la descrizione di analogo requisito presente nel Provvedimento di attuazione PSD (***"Qualora la tecnologia del PSP richieda che tali dati siano rimessi in chiaro su dispositivi intermedi, ciò deve avvenire all'interno di dispositivi sicuri…, oppure nell'ambito di sottoreti chiuse non pubbliche sicure (es: reti aziendali protette"***).

Al **Paragrafo** 2, **Comma** 1 si afferma che ***"…per minimizzare i rischi di furto di identità, l'accesso del cliente a funzionalità di consultazione o l'attivazione di operazioni su rapporti in essere con l'intermediario devono essere soggetti ad una idonea procedura di autenticazione; almeno con riferimento all'operatività a carattere dispositivo, tale procedura deve fare ricorso a sistemi di autenticazione a più fattori tra loro indipendenti ("autenticazione forte")."***
Sul punto, si segnala l'inopportunità di un'applicazione estensiva delle metodologie di "autenticazione forte" a contesti che, come quelli legati all'utilizzo delle carte di pagamento su internet, prevedono standard di sicurezza fra soggetti diversi senza l'utilizzo di tali modalità.

Al **Paragrafo** 3 si afferma che ***"… l'intermediario deve disporre di procedure per assicurare che ogni transazione di pagamento sia eseguita solo previa autorizzazione da parte dell'utente …".***

Risulterebbe utile indicare le relazioni tra il requisito e:

- pagamenti ricorrenti (ad es specificando che il requisito è valido solo nel caso del primo pagamento);
- utilizzo cosiddetto off-line di carte di pagamento (ad es. indicando un limite superiore agli importi);
- pagamenti effettuati da gestori di "portafogli elettronici" (ad esempio, specificando che il requisito è valido solo nel caso della registrazione dello strumento di pagamento, come avviene in *paypal*).

TITOLO V; CAPITOLO 9 -"DISPOSIZIONI IN MATERIA DI CONTINUITÀ OPERATIVA

Il testo in consultazione aggiorna le "Linee guida per le infrastrutture qualificate del sistema dei pagamenti" emanate a novembre del 2004.

Rispetto a tale regolamentazione viene oggi proposto un impianto regolamentare fondato sull'assunto che ***" … il piano si inquadra nella complessiva politica aziendale sulla sicurezza …"*** (cfr. **Titolo** V; **Capitolo** 9; **Paragrafo** 4; **Comma** 4).

Premesso che tale impostazione è in larga parte condivisibile in quanto i sistemi di sicurezza e continuità operativa non possono essere considerati in modo disgiunto, si riterrebbe però opportuno, come nella precedente regolamentazione, menzionare esplicitamente gli adempimenti relativi alla continuità operativa in capo soprattutto agli Organi aziendali.

In tale prospettiva, si segnalano di seguito i principali passi della precedente normativa su cui si riterrebbe utile riflettere:

- ***"La direzione partecipa a tutte le fasi più rilevanti del piano, assicurandone il rispetto ai diversi livelli di responsabilità. Essa attua le misure più idonee per diffondere la conoscenza del piano tra il personale; accerta che gli aspetti più importanti delle principali fasi del piano siano formalmente documentati; riferisce periodicamente agli organi amministrativi e di controllo sugli adempimenti previsti dal piano e sui relativi esiti";***
- ***"il consiglio di amministrazione assicura, in coerenza con le indicazioni formulate nelle richiamate sedi di coordinamento nazionale, che nel piano stesso: a) siano … ";***
- ***"Il consiglio riserva particolare attenzione alla previsione di adeguati meccanismi e procedure di controllo di pertinenza della funzione di revisione interna o di soggetti terzi indipendenti";***
- ***"il consiglio stesso valuta attentamente le possibilità di applicazione di standard di sicurezza riconosciuti a livello nazionale e/o internazionale, nonché l'assoggettamento del piano stesso a valutazione da parte di terze parti ovvero a certificazione eseguita da laboratori di valutazione accreditati presso enti a ciò delegati, ove ciò fosse possibile in base agli standard di sicurezza prescelti"***

- *"ricade nella responsabilità dei vertici aziendali la formulazione delle politiche in tema di continuità operativa e l'approvazione dei relativi piani di sviluppo e di gestione".*

Su un piano più generale, si osserva che quanto previsto dalla norma in esame circa le modalità di accettazione del rischio residuo (devono *"essere accettati dall'intermediario"*) non risponde pienamente all'affermata consuetudine di richiederne l'accettazione da parte dell'Organo con funzione di supervisione strategica.

Più in particolare, le precedenti istruzioni in merito alla continuità operativa prevedevano i seguenti passi:

"4.1 Ruolo dei vertici 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.
Il consiglio di amministrazione 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'alta direzione 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."

Si rileva, inoltre, che nelle nuove Istruzioni di Vigilanza non sono più previsti i riferimenti presenti nella precedente disciplina che recitava, nella parte generale di introduzione alle tematiche al punto 2: *"Le altre banche, tenute a completare gli adempimenti entro il citato termine del 31 dicembre 2006, vorranno valutare l'opportunità di adottare soluzioni di continuità operativa coerenti con gli standard definiti nell'ambito degli organismi di categoria".*

La definizione di "standard definiti nell'ambito degli organismi di Categoria" nel caso delle BCC-CR ha sinora permesso di portare a fattore comune una serie di attività (ad esempio la *Business Impact Analisys*, la definizione di politiche strategiche, la formalizzazione del Piano di Continuità e delle modalità dei test) che consentivano, nel rispetto del principio di proporzionalità, di rendere maggiormente efficiente il processo di adeguamento allo standard.
Si richiede pertanto di poter riproporre tale riferimento nel corpo normativo delle nuove Istruzioni di Vigilanza al fine di ridurre l'impatto determinato dalle attività sopra esposte in capo ad ogni singola BCC-CR.

Tale riferimento potrebbe inoltre, qualora non fosse accolta la richiesta di riformulazione dei criteri relativi alle *best practice* illustrata al paragrafo 5, essere esteso anche all'applicazione delle componenti previste dalla norma definendo un set minimo di attività condivise a livello nazionale ed applicato (anche in forma proporzionalmente limitata) da tutte le banche di piccole dimensioni.

5. Definizione di procedure di allerta

Si esprime preoccupazione con riguardo **all'onerosità sottesa alla messa in opera di quanto richiesto in intermediari caratterizzati da ridotti profili organizzativi, evidenziando a riguardo un elevato rischio di contemporanee ridondanza e inefficacia** delle procedure citate.

Si rappresenta come, al momento, le BCC-CR che hanno adottato il modello 231/01 dispongano di un protocollo per la gestione delle informazioni nei confronti dell'Organismo di Vigilanza che prevede la possibilità di segnalare a tale Organismo, con garanzia di riservatezza, violazioni o sospetti di violazione rispetto al modello 231/01.
Le BCC-CR, inoltre, adottano codici etici che tra le tante previsioni in ordine ai corretti comportamenti aziendali, impongono ai dipendenti la segnalazione agli organi aziendali di qualunque irregolarità riscontrata.

Ad oggi, nella generalità delle BCC-CR, **non è definito un processo per la gestione delle segnalazioni, né un sistema di tracciamento e conservazione delle stesse** e **gli oneri di relativa messa in opera risulterebbero estremamente elevati**.

Pur nella consapevolezza dell'utilità potenziale che l'implementazione di procedure formalizzate di allerta interna potrebbe assumere con riguardo al presidio dei rischi di non conformità e di frode, si ritiene che l'introduzione di un obbligo a riguardo, in particolare per le piccole banche locali, dovrebbe essere valutato con estrema cautela sia in ordine alla già commentata prevedibile onerosità di impianto - a fronte, peraltro, di vantaggi informativi non valutabili - sia tenuto conto del peculiare contesto operativo di riferimento, data la dimensione locale.

Si chiede, pertanto, di non disciplinare l'obbligo di adozione delle procedure in argomento per gli intermediari minori (ipotesi H0), permettendo con ciò la possibilità per il Sistema del Credito Cooperativo di darsi in via autoregolamentare una disciplina in proposito, valutatene adeguatamente e nel tempo le migliori modalità realizzative e le connesse implicazioni.

Ciò posto, si ritiene comunque necessario che le disposizioni a riguardo siano opportunamente calibrate e declinate per poterne supportare l'implementazione da parte degli intermediari nel pieno rispetto delle proprie specificità organizzative e del complessivo quadro normativo di riferimento (ivi incluse le disposizioni in materia di *privacy*) .

Nel rinviare, per una maggiore articolazione in proposito, ai commenti riportati al punto 4 della successiva sezione "***Risposte ai quesiti posti dalla Banca d'Italia***", a titolo esemplificativo si evidenzia, in particolare, la necessità di fornire indicazioni in merito alle attribuzioni ritenute percorribili, alla luce del peculiare profilo di responsabilità sotteso, con riferimento al ruolo responsabile di sceverare le informazioni fornite dai dipendenti per determinare quali, essendo rilevanti, debbano essere sottoposte agli organi aziendali (la cui attribuzione non è precisata nel documento di consultazione).

6. Ampliamento del perimetro di riferimento della compliance

Tra le novità di rilievo del documento rientra certamente l'attribuzione alla funzione di conformità dell'attività aziendale alle normative di natura fiscale per evitare di incorrere in violazioni o elusioni di tali norme ovvero in situazioni di abuso del diritto delle stesse previsioni.
La normativa fiscale ha indubbia rilevanza per le implicazioni che discendono da una sua eventuale violazione. Le problematiche di carattere fiscale possono infatti impattare in modo rilevante in termini di perdite, di reputazione e di salvaguardia della fiducia del pubblico.

Pur nella consapevolezza dell'importanza che, con riguardo a tali tematiche, l'intero sistema organizzativo della banca sia improntato alla **prevenzione del rischio** piuttosto che alla tempestività dell'intervento correttivo, non si può non esprimere preoccupazione in merito all'onerosità, in particolare per gli intermediari minori, della **richiesta di incardinare in capo alla funzione di *compliance* la verifica della conformità dell'attività aziendale alle normative di natura fiscale**.

Preliminarmente si evidenzia, a tale riguardo, come nel disegno di legge delega A.C. 5291, attualmente all'esame al Parlamento, 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 sia contemplata solo per i soggetti di maggiori dimensioni.

Si rappresenta l'opportunità di disporre, per gli intermediari minori, la facoltatività dell'inserimento in capo alla funzione di *compliance* della verifica di conformità dell'attività aziendale alle normative di natura fiscale e di declinare nel testo delle disposizioni, con riguardo alle soluzioni organizzative per strutturare adeguati presidi a fronte del rischio di non conformità alla disciplina fiscale, la necessaria libertà organizzativa per gli intermediari,

prevedendo a riguardo la possibilità di porre in essere forme di collaborazione tra la funzione specialistica tributaria, ovunque allocata, e la funzione *compliance*, che non risulta nella generalità dei casi dotata del necessario bagaglio di conoscenze specialistiche richieste.

Nell'ottica di garantire efficacia ed efficienza delle soluzioni di conformità adottate dagli intermediari, dato anche lo specifico profilo competenziale necessario, nonché in linea con il principio di proporzionalità, l'autonomia in materia di connesse scelte organizzative lasciata agli intermediari dovrebbe, nella sostanza, permettere anche di non includere espressamente nel novero delle aree normative necessariamente e totalmente allocate sotto la responsabilità, della funzione compliance, la disciplina fiscale. Le soluzioni organizzative per innalzare il livello di presidio richiesto con riguardo a tali norme potrebbero basarsi su una responsabilità limitata alla fase di disegno del *framework* di gestione del connesso rischio di non conformità (ed eventualmente alla sua periodica verifica). Alla funzione specialistica 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).

Si evidenzia a riguardo come nella generalità dei casi, dati i ridotti profili dimensionali, nelle BCC-CR non è presente un fiscalista interno, in quanto la funzione è delegata alle strutture federative che la assolvono per conto delle associate sulla base dei riferimenti interpretativi e delle modalità applicative definite a livello di sistema. Tale circostanza assicura la piena indipendenza della funzione fiscale e il suo operare secondo criteri e best standard trasparentemente e correttamente applicati.
Una completa e adeguata copertura del rischio di non conformità alla disciplina fiscale si realizzerebbe, quindi, attuando soluzioni organizzative e procedurali focalizzate su:

- prevenzione delle irregolarità gestionali che potrebbero tradursi in violazioni tributarie, incidendo sull'efficacia dei processi di condivisione delle informazioni non solo in fase operativa, ma anche in fase decisionale;
- un'adeguata formazione anche in materia tributaria del personale aziendale, a tutti i livelli.

Si manifesta, a riguardo, la disponibilità a confrontarsi sui presidi già adottati per la gestione e il controllo del rischio di non conformità alle norme fiscali - per valutarne la coerenza con le esigenze dell'organo di vigilanza - e sulle iniziative ulteriori da intraprendere.

Si ritiene che i costi di adeguamento alle previsioni come attualmente definite, pur mitigabili dal ricorso a soluzioni di sistema, **sarebbero molto elevati**.

Si evidenziano, infine, perplessità in merito alla definizione "estensiva" che il documento introduce, con riguardo ai "***rischi derivanti dal coinvolgimento in operazioni fiscalmente irregolari poste in essere dalla clientela"***, con il rischio, laddove non opportunamente chiarita, di improprie implicazioni di ruolo degli intermediari bancari. Si chiede a riguardo di

fornire una declinazione atta ad adeguatamente circoscrivere e individuare i profili ritenuti rilevanti.

7. Obbligo di formalizzare il processo di valutazione delle attività aziendali e di dotarsi di processi e metodologie di valutazione delle attività, anche a fini contabili, affidabili e integrati con il processo di gestione del rischio

Pur condivisibile nelle finalità, anche tenuto conto di come l'esperienza della crisi ha reso ulteriormente evidente la necessità di disporre di un valido modello di riferimento per identificare, valutare e gestire i rischi in modo efficace, non si può non esprimere preoccupazione per la complessità e onerosità che l'evoluzione verso un modello di *enterprise risk management*, così evidentemente sotteso a diversi contenuti dispositivi, riveste per intermediari minori.

Si chiede a riguardo di prevedere, in ossequio al principio di gradualità, un'adeguata flessibilità dei tempi di implementazione relativi per permettere la definizione e attuazione delle iniziative, a livello di Sistema, necessarie per supportare l'adeguamento delle banche di Categoria.

8. Compiti e collocazione delle funzioni di controllo

RISK MANAGEMENT FUNCTION (RMF) – COMPITI E COLLOCAZIONE ORGANIZZATIVA

Nel quadro complessivo assolutamente condivisibile del **rafforzamento** del ruolo della **funzione di controllo rischi**, si ritiene fondamentale una rivisitazione di uno degli elementi connessi all'indipendenza (Cfr. paragrafo 3.3, in cui viene inserito il concetto di "**dirette dipendenze"** dagli organi di vertice) che appare improntato a una eccessiva rigidità organizzativa e suscettibile di alcuni effetti collaterali sull'operatività della funzione non reputati opportuni.

Capitolo 7, Sezione 3, Paragrafo 3.3: "Al fine di rafforzarne l'indipendenza, 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. Nota 22: ***Le banche classificate, a fini SREP, nelle macro-categorie 1 e 2 (cfr. Circolare 269 del 7 maggio 2008, "Guida per l'attività di vigilanza", Sezione I, Capitolo I.5) collocano obbligatoriamente la funzione di controllo dei rischi alle dirette dipendenze del comitato controllo e rischi, ove costituito, o dell'organo con funzione di supervisione strategica".***

Si ritiene che nell'esercizio delle proprie prerogative la RMF, nell'ambito dell'organizzazione aziendale, sia il principale referente in materia di rischi dell'Organo con Funzione di Gestione

ed allo stesso tempo svolga per detto Organo un "ruolo di garanzia" nell'interlocuzione e nell'iterazione ordinaria con le strutture operative e di business: l'indipendenza della RMF dalle strutture operative e di business le consente di esercitare tale ruolo concretizzando in tal modo il concetto di "funzione di controllo di secondo livello" ed allo stesso tempo assicurando l'efficacia dell'azione in quanto parte integrante della complessiva fase esecutiva. In modo analogo la Revisione Interna svolge lo stesso "ruolo di garanzia" verso l'Organo con funzione di Supervisione Strategica: l'indipendenza della Revisione Interna dall'Organo con funzione di Gestione e quindi dalla complessiva fase esecutiva della quale fanno parte sia le strutture operative e di business sia le funzioni di controllo di secondo livello le consente di esercitare tale ruolo concretizzando in tal modo il concetto di "funzione di controllo di terzo livello" ed allo stesso tempo assicurando l'efficacia dell'azione in quanto *committed* dall'Organo con funzione di Supervisione Strategica.

Ad ulteriore supporto delle argomentazioni sopra rappresentate, si ritiene che il principio dell'efficacia dell'azione delle Funzioni di Controllo debba assumere, in un contesto di evoluzione della disciplina in materia di controlli ed alla luce dei riscontri degli ultimi anni, primaria rilevanza. L'efficacia è strettamente collegata all'integrazione della RMF nella organizzazione aziendale richiamando un concetto di *risk management* quale processo aziendale che coinvolge, in una logica sia top-down sia bottom-up, tutta la struttura: unità commerciali, funzioni di controllo, manager, organi di vertice.
La collocazione organizzativa della RMF a tale proposito costituisce il principale fattore di successo od insuccesso della Funzione dal punto di vista dell'efficacia della sua azione. L'eccessiva distanza, al limite indipendenza, dalla fase esecutiva, eventualmente attenuata da un coinvolgimento formale in momenti istituzionali, che si avrebbe riportandola alle dirette dipendenze dell'Organo con Funzione di Supervisione Strategica, ne potrebbe attenuare il sostanziale apporto e contributo per un'assunzione e gestione dei rischi sempre più ponderata e consapevole, sviluppati all'interno di una fase esecutiva al cui vertice figura l'Organo con Funzione di Gestione.
Si richiede pertanto che per la RMF sia prevista la possibilità, indipendentemente dalla classe SREP di appartenenza, di poter collocare la funzione alle dirette dipendenze dell'Organo con Funzione di Gestione.
In ultimo si rappresenta che pare non coerente la collocazione organizzativa indicata con quanto previsto nello stesso schema di disciplina in materia di nomina e revoca dei responsabili delle Funzioni di Controllo: ***Capitolo 7, Sezione 3, Paragrafo 1 "i responsabili 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"***

RISK MANAGEMENT FUNCTION (RMF) E FUNZIONE DI CONFORMITÀ (FC) – SEPARATEZZA ORGANIZZATIVA

Capitolo 7, Sezione 3, Paragrafo 1: "le funzioni aziendali di controllo siano tra loro separate, sotto un profilo organizzativo. I rispettivi ruoli e responsabilità devono essere formalizzati;"

"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;".

Nel documento in consultazione viene proposta quale *first best* la separatezza tra RMF e FC lasciando agli intermediari la possibilità di applicare il principio di proporzionalità nel caso in cui intendano optare per una convergenza organizzativa tra le due funzioni. Il richiamo al principio di proporzionalità sottende un'idea di *second best* nella quale, a condizione che sia salvaguardata l'efficacia dei presidi, è concesso, in ragione di minori dimensioni e complessità operativa, di sviluppare soluzioni organizzative di entità ridotta, dunque meno onerose ma implicitamente considerate inferiori alle soluzioni ritenute ottimali e comunque non adeguate nei casi di maggior dimensione o complessità operativa.

Le funzioni RMF e FC appartengono entrambe all'area dei controlli di secondo livello e come anche evidenziato in diversi passaggi del documento di consultazione, l'area dei Rischi Operativi della RMF e l'area di competenza della FC presentano "***forti interrelazioni***". Ferma restando la separatezza con la Revisione Interna, inquadrata nell'area dei controlli di terzo livello, si ritiene che le interrelazioni suddette tra RMF, con particolare riferimento ai Rischi Operativi, e FC siano tali da non far escludere quale *first best* l'ipotesi di convergenza organizzativa:

- analoghe caratteristiche del framework metodologico di identificazione, valutazione, monitoraggio e controllo;
- continuità, in taluni casi e sotto certi aspetti, sovrapposizione del profilo di rischio presidiato;
- riferimenti operativi e di *governance* aziendali analoghi nella dialettica volta ad un innalzamento dei livelli di presidio (mitigazione): organizzazione e processi, risorse umane, IT;
- riconduzione a corpo unico sotto il presidio del CRO di tutti i rischi aziendali.

Quanto precede indipendentemente dalla dimensione o dalla complessità operativa dell'intermediario.
Si richiede pertanto di riconsiderare il vincolo dell'applicabilità del principio di proporzionalità (la cui definizione puntuale potrebbe conseguentemente non renderlo applicabile ad intermediari di dimensione e complessità operativa sopra la soglia definita) nella scelta organizzativa relativa alle funzioni di controllo di secondo livello: RMF e FC entrambe a riporto del CRO *vs* separatezza organizzativa.
Ove le suddette considerazioni non siano accolte si richiede che siano specificati i *driver* alla base della valutazione di *first best* prudenziale dell'ipotesi di separatezza organizzativa tra le due funzioni al fine di poter valutare puntualmente gli elementi di attenuazione del presidio nel caso in cui, ricorrendo i presupposti di proporzionalità, si optasse per una soluzione di

convergenza. Tali informazioni costituirebbero peraltro l'utile supporto al processo decisionale che interesserà gli Organi Aziendali nella scelta dell'assetto organizzativo.

Risk Management Function (RMF) e Funzione di Conformità (FC) – Programmazione e Rendicontazione

Capitolo 7, Sezione 3, Paragrafo 2: "In particolare: 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;".

"Al termine del ciclo gestionale, con cadenza quindi annuale, le funzioni aziendali di controllo: - presentano agli organi aziendali una relazione dell'attività svolta, che illustra le verifiche effettuate, i risultati emersi, i punti di debolezza rilevati e propongono gli interventi da adottare per la loro rimozione; - riferiscono, ciascuna per gli aspetti di rispettiva competenza, in ordine alla completezza, adeguatezza ed affidabilità del sistema dei controlli interni.".

La previsione normativa in questione definisce degli obblighi fondati su principi di funzionamento mutuati dalla Revisione Interna (ed estesi quale prassi operativa alla Funzione di Conformità) non tenendo invece conto delle diversità che contraddistinguono la modalità di espletamento dell'attività di risk management. La Revisione Interna di norma opera definendo un piano di attività con copertura evidentemente parziale per ciascun ciclo di gestione delle diverse aree di processo e rischio ed in esito alle stesse produce *deliverable* per ciascun task di piano consuntivabili in modo naturale in una relazione complessiva di fine ciclo. La copertura completa delle aree di processo e di rischio si realizza di norma in un orizzonte pluriennale.

Il Risk Management invece è chiamato ad operare all'interno di un *framework* metodologico ed operativo che deve assicurare **nel continuo** la copertura di **tutte le aree di processo e di rischio**.

Per tale ragione la normativa interna definisce non solo ruolo e responsabilità ma anche i compiti, e dunque le attività svolte dalla RMF per ciascun ambito operativo (di processo) e ciascun ambito funzionale (di rischio). La normativa interna che regolamenta i compiti della RMF è definita dall'Organo con Funzione di Gestione ed approvata dall'Organo con Funzione di Supervisione Strategica, in fase d'impianto ed in fase evolutiva / correttiva per tener conto dei mutamenti di contesto gestionale, di mercato, regolamentare. Detta normativa assurge a ruolo di Programmazione delle attività ordinarie. Nel caso invece di attività straordinarie programmabili (dunque di norma di tipo "progettuale") è evidente che si applichi alla RMF quanto previsto per ogni altra funzione aziendale e che dunque tali interventi debbano essere rappresentati in un documento di programmazione annuale da presentare agli Organi Aziendali (il tutto di norma è parte integrante della Pianificazione).

Si richiede pertanto che nella disciplina delle attività di Programmazione siano effettuati gli opportuni distinguo per la RMF che tengano conto delle modalità con le quali essa realmente opera, nell'ottica di efficacia della sua azione ma anche di efficienza con cui la stessa deve essere svolta.

9. ECCESSIVO AFFIDAMENTO SUI RATING ESTERNI

Non possiamo non condividere l'obiettivo, richiamato nelle disposizioni in consultazione, di limitare l'eccessivo affidamento delle banche sui giudizi delle agenzie di *rating*, le cui decisioni e valutazioni seguono sempre a distanza i movimenti dei mercati. Ciò anche alla luce dell'evidente conflitto di interessi in cui tali agenzie operano.
Ciò a nostro avviso non deve, tuttavia, tradursi in incrementi ingiustificati degli oneri operativi a carico delle banche più piccole. Il principio di proporzionalità, peraltro correttamente richiamato nel testo in consultazione, dovrebbe essere opportunamente declinato a riguardo, consentendo alle piccole banche flessibilità sufficiente tra le diverse metodologie previste nel quadro di Basilea 2 e lo sviluppo e l'utilizzo di metodologie interne coerenti con il proprio modello di *business* e non eccessivamente complesse (quali quelle sottese ai modelli "*internal rating based*" - IRB).

Risposte ai quesiti posti dalla Banca d'Italia

1. Valutazione delle attività aziendali

Q1. A quali caratteristiche attualmente risponde nella vostra istituzione il processo di valutazione delle attività aziendali?

L'applicazione dei principi contabili internazionali già obbliga di fatto le banche a dotarsi di processi e metodologie di valutazione delle attività aziendali. Si tratta però, nella generalità dei casi, ancora di un "adempimento" per le banche del quale non vengono colte le ricadute in termini di supporto strategico/operativo, di gestione del rischio e neppure le opportunità di valorizzazione in un'ottica sinergica.

Q2. Le metodologie di valutazione sono testate sotto scenari di stress?

Si, come previsto dalla normativa.
Lo scarso collegamento con i processi di definizione delle strategie e di gestione del rischio, può però ridurre l'attività ad un esercizio accademico.

Q3. Quali sarebbero i costi addizionali da sostenere per la formalizzazione del processo di valutazione secondo le caratteristiche definite dalla normativa?

Lo sviluppo e la formalizzazione del processo di valutazione secondo le indicazioni della nuova proposta normativa comporterebbe sicuramente costi **molto elevati**, anche tenuto conto dell'effetto di mitigazione conseguibile operando a livello di Sistema del Credito Cooperativo.

Ipotesi di sviluppo

Volendo ipotizzare un possibile percorso evolutivo, operando come Sistema del Credito Cooperativo si dovrebbe:

a. armonizzare[2] (non omologare, ma rendere confrontabili) i differenti sistemi di

[2] Con il termine armonizzare si intende sintetizzare un processo volto a:
- censire i differenti sistemi di valutazione,
- classificarli in funzione delle caratteristiche specifiche e dell'ambito di applicazione,
- esplicitare le ragioni per cui a fronte di un medesimo oggetto da valutare si possano/debbano utilizzare sistemi diversi di valutazione (con conseguenti differenti risultati),
- evidenziare punti di congruenza/divergenza tra i sistemi stessi.

L'obiettivo è dunque disporre di una mappa articolata da utilizzare come strumento di orientamento/razionalizzazione sia nel processo di valutazione, sia nella lettura/utilizzo degli output del processo stesso.

valutazione;

b. sviluppare la gamma di indicatori / metodologie utilizzabili per il processo di valutazione, al fine di poter rappresentare una molteplicità di scenari e migliorare le attività di stress test;
c. ampliare le fonti informative di riferimento, anche attraverso una sistematizzazione delle componenti qualitative;
d. avviare un articolato piano di formazione per le funzioni di gestione e gli organi di governo, per accrescere le capacità di lettura e utilizzo di dette metodologie, da affiancare a iniziative permanenti di riflessione in merito all'evoluzione dello scenario complessivo (contestualizzazione).

Quanto delineato attiene essenzialmente al secondo item delle richieste avanzate dalla nuova disciplina.

La scelta di operare a livello di sistema dovrebbe comunque consentire di :

- assolvere alla richiesta di processi di valutazione basati su due unità differenti per la definizione e la validazione delle metodologie (primo item),
- facilitare la separatezza e indipendenza delle unità di valutazione ed i responsabili della negoziazione (terzo item).

Ruolo delle strutture associative

- coordinare/sviluppare il progetto di studio e adeguamento (con riguardo ai punti a,b,c);
- predisporre un piano di formazione per tutte le funzioni coinvolte nel processo di adozione e utilizzo delle nuove metodologie;
- fornire consulenza/assistenza alle banche nel processo di valutazione delle attività aziendali

2. Risk appetite framework

Q4. **La vostra istituzione si è dotata di un formale risk appetite framework? In caso positivo, quali sono gli organi coinvolti? Sono utilizzate variabili quali-quantitative?**

Nella generalità dei casi, non esiste un formale *risk appetite framework*. Attualmente in alcuni ambiti territoriali le BCC-CR dispongono di una politica generale dei rischi e, nella generalità dei casi - sempre, di politiche del credito e di politiche della finanza, che fissano limiti quali/quantitativi all'assunzione dei rischi.

In diversi casi, le BCC-CR si avvalgono di una metodologia, applicata nella definizione dei Piani Strategici da circa 3 anni, che utilizza in sede di programmazione quantitativa e di verifiche di sostenibilità in ottica ICAAP rischi/capitale, sia il concetto di *risk tolerance*, sia il concetto di *risk appetite*[3].

Q5. **Quanto ritenete costerebbe l'implementazione di un *risk appetite framework*? L'utilizzo di variabili quali-quantitative avrebbe effetti sui costi?**

Anche accogliendo la metodologia di vigilanza descritta nel seguito, nei commenti al BOX 1, i **costi** risulterebbero **elevati** in quanto non si tratterebbe solo di perfezionare policy eventualmente già adottate dalla banca o assicurarne l'adozione da parte di banche che al momento non applichino i riferimenti richiamati, pervenendo ad una formalizzazione della soglia di tolleranza e del parametro di appetito al rischio, ma anche di implementare procedure, strumenti e applicativi informatici atti a migliorare la predisposizione e il monitoraggio degli indicatori di riferimento e la loro traduzione in vincoli e incentivi per la struttura aziendale.

Ipotesi di sviluppo

Come sopra indicato, per consentire l'implementazione di un *risk appetite framework* si renderebbe necessario predisporre procedure strumenti e metodi atti a facilitare le BCC-CR nel:

a) processo di determinazione della propria soglia di tolleranza e del parametro di appetito al rischio;
b) elaborazione di riferimenti e procedure per la traduzione in vincoli e incentivi per la struttura aziendale;
c) percorso di adeguamento/perfezionamento delle policy adottate e dei conseguenti regolamenti, procedure, strumenti e applicativi informatici, ….

Ruolo delle strutture associative

- predisporre quanto descritto nel precedente paragrafo;
- definire un piano di formazione per tutte le funzioni coinvolte nel processo di adozione e utilizzo delle nuove metodologie;

[3] Nel documento di consultazione si definisce come *risk tolerance* il "livello assoluto di rischio" mentre il *risk appetite* viene definito come "limite effettivo" del rischio stesso. Da evidenziare che in letteratura si definisce come "rischio accettabile l'ammontare del rischio che una società è disposta ad accettare nel perseguire la sua missione" mentre la "tolleranza al rischio" viene definita come la misura consentita di variazione o di scostamento rispetto all'obiettivo da realizzare. (cfr ERM – Modello di riferimento e alcune tecniche applicative – AIA e PriceWaterhouseCoopers 2006. Del resto a fronte di evidenti difformità tra supervisori e tra questi e l'industria sul significato da attribuire a tali espressioni, queste vengono sovente impiegate come sinonimi. (BCBS- *Principles for enhancing corporate governance* – ottobre 2010). In considerazione di ciò appare opportuno richiedere un'esplicitazione dei significati sottesi alle due espressioni

- fornire consulenza/assistenza alle banche nel processo di valutazione delle attività aziendali.

BOX 1

Determinazione della tolleranza al rischio / appetito per il rischio

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.

Coerentemente con il principio di proporzionalità, si ritiene che per le banche di ridotte dimensioni e minore complessità operativa, come le BCC-CR, sia opportuno attenersi all'individuazione di parametri già 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.

Nella metodologia applicata ai Piani Strategici da diverse BCC-CR, l'appetito per il rischio è definito secondo logiche ICAAP, in termini di rapporto massimo tra rischi e capitale complessivo della Banca, in sostanza quindi come l'ammontare massimo di capitale che si intende porre a copertura dei rischi a fronte di un determinato rendimento atteso.

Dove i rischi sono generalmente misurati in termini di requisiti patrimoniali riferiti ai rischi di primo pilastro e il capitale complessivo in termini di patrimonio di vigilanza. Al numeratore la misura dei rischi può peraltro ricomprendere anche i capitali interni riferiti ai rischi di secondo pilastro e all'ulteriore capitale interno assorbito dagli stress test.

Difficoltà di carattere metodologico si evidenziano nell'elaborazione di una misura complessiva di propensione al rischio che vada a compendiare al proprio interno rischi non omogenei per modalità di misurazione.

In generale si ha quindi:

- **risk appetite (statico) = max (Rischi / Capitale)**

Una tale definizione permette di considerare in un'ottica perfettamente coerente con quella ICAAP l'esposizione ai rischi della BCC-CR e definire rispetto a tale esposizione quale sia il buffer minimo percentuale di capitale non allocato.

L'indicatore può essere quindi articolato in termini di sue componenti riferite ai singoli rischi, ad esempio:

- **risk appetite rischio di credito (statico) = max. (Rischio di Credito / Capitale)**

- **risk appetite rischio di tasso (statico) = max (Rischio di Tasso d'Interesse / Capitale)**
- **…**
- **risk appetite rischio di concentrazione (statico) = max (GA / Capitale)**

Soprattutto per quanto riguarda il rischio di credito, il risk appetite può essere ulteriormente scomposto in termini di singole componenti del numeratore riferite ai singoli rischi, ad esempio (*corporate*, *retail*, mutui ipotecari con garanzie ammissibili, ecc.).

L'indicatore viene utilizzato per programmare una dinamica dei rischi coerente con quella del capitale che rispetti il livello assoluto di rischio che la Banca è a priori disposta ad assumere.

Esso è utilizzabile anche per programmare in chiave dinamica le evoluzioni dei rischi e del capitale per conseguire un target desiderato in termini di rapporto rischi/capitale.

Laddove sia necessario un **rafforzamento della posizione patrimoniale** la relazione dinamica tra rischi e capitale sarà programmata in misura tale che la variazione percentuale dei rischi risulti inferiore a quella del capitale evidenziando un *risk appetite* dinamico (derivata rischi/capitale) inferiore a 1:

risk appetite (dinamico) = var% Rischi / var% Capitale < 1

Laddove sia appropriato un **mantenimento dell'attuale posizione patrimoniale** la relazione dinamica tra rischi e capitale sarà programmata in misura tale che la variazione percentuale dei rischi risulti uguale a quella del capitale evidenziando un risk appetite dinamico (derivata rischi/capitale) pari a 1:

risk appetite (dinamico) = var% Rischi / var% Capitale = 1[4]

Va sottolineato che il risk appetite così definito **non considera il rischio di liquidità**, avendo tale rischio una propria autonoma definizione di tolleranza come previsto nella policy di liquidità del Credito Cooperativo.

3. Risk management function

Q6. **E' già prevista un'azione di controllo preventivo della RMF nella vostra istituzione?**

[4] Laddove sia auspicabile (nel caso di indici di patrimonializzazione particolarmente elevati) un **indebolimento della posizione patrimoniale** la relazione dinamica tra rischi e capitale sarà programmata in misura tale che la variazione percentuale dei rischi risulti superiore a quella del capitale evidenziando un risk appetite dinamico (derivata rischi/capitale) superiore a 1:

risk appetite (dinamico) = var% Rischi / var% Capitale > 1

Nella generalità dei casi, nelle BCC-CR l'azione di controllo preventivo, in termini di analisi a supporto della direzione generale, viene svolta solo in rari casi.

Q7. Come valutate la possibilità di riconoscere un tale ruolo alla RMF?

La valutazione è nel complesso positiva, in quanto si rafforza il ruolo della funzione, consentendo di portare maggiori informazioni e analisi di impatto preventivo delle scelte gestionali agli organi di verti.ce.

Va tuttavia evidenziato che l'applicazione di tale previsione normativa nelle banche di piccole dimensioni potrebbe risultare poco efficace e di difficile attuazione a causa, ad esempio, dell'attribuzione di un non sempre adeguato livello di autorevolezza e della carenza di esperienze e conoscenze adeguate.

Q8. Ritenete che ci siano rischi di attuazione?

Sì, potrebbe determinarsi una situazione di conflitto tra gli organi aziendali, un rallentamento delle attività, nonché il rispetto puramente formale della previsione normativa in questione.
La preliminare e puntuale individuazione di un numero ristretto di OMR potrebbe, in parte, ridurre le debolezze di cui sopra.

Q9. Quali sarebbero i costi di una tale previsione?

Costi elevati dovuti a:
- formazione e inquadramento contrattuale della risorsa incaricata;
- individuazione delle OMR;
- indiretti, legati al coinvolgimento nelle valutazione delle ORM delle RMF;
- eventuale ricorso a servizi di consulenza.

BOX 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, paragrafo 3.3)

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

Preliminarmente si esprime condivisione per un impianto sulla cui base i **criteri** per la identificazione delle operazioni di maggior rilievo sono **autonomamente individuati dalla singola banca.**

Si esprime altresì la convinzione che il parere preventivo della Funzione di controllo dei rischi integri il processo decisionale inerente le operazioni di maggiore rilievo – OMR - arricchendone la visione dialettica.

Le OMR dovrebbero essere identificate nelle iniziative/operazioni che modificano l'operatività della banca quali:

- operazioni di intermediazione o investimento che modificano l'equilibrio economico/patrimoniale, misurato secondo logiche ICAAP (cfr. box1),
- operazioni straordinarie, cessioni /aperture di sportelli e aperture di sedi distaccate,
- contratti di outsourcing, operazioni di re-internalizzazione, scelte in materia di continuità operativa,
- deroghe a parametri qualitativi previsti nelle singole policy (credito, portafoglio di proprietà, ecc.).

Ipotesi di sviluppo

In via preliminare va osservato che nelle disposizioni, con riguardo a tale tematica, viene dato per scontata l'esistenza presso tutti gli intermediari (ivi comprese le BCC-CR) di una specifica RMF e chiesto di conoscere se tale funzione già svolge azioni di controllo preventivo sulla coerenza delle operazioni di maggior rilievo con la politica aziendale di governo dei rischi.

La costituzione di una funzione separata in banche di dimensioni contenute e di limitata complessità operativa determinerebbe un notevole impatto sotto il profilo della *governance*, organizzativo ed economico, soprattutto laddove fosse collocata alle dirette dipendenze del Consiglio di Amministrazione

Inoltre, tenuto conto delle attività preventive e continuative che la funzione è chiamata a svolgere (quale ad esempio la formulazione di pareri preventivi sulle operazioni di maggior rilievo), della prevista interazione continua con le unità di business e in considerazione della necessità di mantenere le competenze tecniche e gestionali necessarie per re-internalizzare, appare difficilmente immaginabile un'esternalizzazione efficace della funzione a soggetti terzi.

Risulta invece preferibile l'ipotesi di accorpamento della funzione di conformità e di controllo del rischio residenti in banca in un'unica funzione (soprattutto nelle BCC-CR di piccole o medie dimensioni) supportata dalle strutture associative. L'accorpamento delle funzioni comporta infatti sia la riduzione degli oneri economici, sia una maggiore efficienza tra gli attori del processo di gestione del rischio.

Ruolo delle strutture associative

In caso di OMR le BCC-CR, come già accade per determinate operazioni straordinarie, potrebbero fare ricorso al supporto della Federazione e di altri soggetti del sistema a rete, nell'ambito delle rispettive competenze.
Le strutture associative parteciperanno alla definizione di strumenti e metodologie per supportare la RMF e potrebbero predisporre specifici percorsi di formazione sia per la struttura di RMF, sia per le funzioni e gli organi aziendali interessati dalla sua attività.

4. Procedure di internal alert

Q10 **Come valutate la possibilità di implementare una procedura di Internal alert nella vostra istituzione?**

Le BCC-CR che hanno adottato il modello 231/2001 dispongono di un protocollo per la gestione delle informazioni nei confronti dell'Organismo di Vigilanza - OdV), che prevede la possibilità di segnalare all'OdV, con garanzia di riservatezza, violazioni o sospetti di violazione al modello 231/2001.
Ad oggi non è definito un processo per la gestione delle segnalazioni, né un sistema di tracciamento e conservazione delle stesse.
L'adozione della procedura potrebbe avere un impatto positivo ma avrebbe certamente costi molto significativi e complessità realizzative peculiari per le BCC-CR oltre a dover essere

attentamente valutato in ordine alle implicazioni che potrebbe avere alla luce della dimensione operativa locale.

Q11 **Quali ritenete dovrebbero essere i requisiti minimi di tali procedure per garantire segnalazioni efficaci, tutela della privacy e del soggetto che effettua la segnalazione?**

Le procedure dovrebbero assicurare che **le segnalazioni siano effettuabili potenzialmente da tutti i dipendenti, circoscrivere adeguatamente i temi e contenuti passibili di segnalazione, prevedere la sola forma scritta, disciplinare un corredo documentale a supporto della segnalazione, ove applicabile**.

Dovrebbero, quindi , tra l'altro essere definiti preventivamente:

- i criteri per l'identificazione delle operazioni e degli eventi da segnalare nonché dei soggetti oggetto di segnalazione;
- le modalità operative per garantire la riservatezza del soggetto segnalante;
- il soggetto destinatario della segnalazione;
- il soggetto incaricato di sceverare le segnalazioni rilevanti in vista della loro sottoposizione agli organi aziendali (sulla base dei criteri normativamente individuati con riguardo all'attribuzione di tale ruolo responsabile);

L'adozione di un sistema di allerta interna, nelle BCC-CR, **potrebbe risultare inefficace oltre che inefficiente a meno di prevedere tra i destinatari della segnalazione, oltre al Presidente del Collegio Sindacale, soggetti esterni quale, ad esempio, il responsabile della revisione interna esternalizzata.**

Q12. **Quali sarebbero i costi di una tale previsione, nelle due opzioni H1 e H2?**

H1: le banche hanno la **facoltà** di definire procedure di allerta interna: costi elevati

H2: le banche **sono tenute** a formalizzare procedure di allerta interna costi molto elevati

Ruolo delle strutture associative

- individuare soluzioni organizzative e procedurali concretamente applicabili;
- predisporre procedure e protocolli modello;
- sviluppare un piano formativo;
- fornire assistenza/consulenza nell'applicazione delle nuove regole.

5. Analisi del rischio informatico

Q 13 **Disponete di un processo formale di analisi del rischio informatico?**

Nelle BCC-CR, no nella generalità dei casi.

Q14 **In caso negativo, quali sarebbero gli effetti sui costi?**

Costi molto elevati, soprattutto per l'implementazione iniziale.

Q15 **Oltre a costi per la formazione di personale specializzato e a costi di consulenza quale altra categoria di costo ravvisate?**

Costi per:

- strumenti per la rilevazione e l'analisi delle informazioni;
- ampliamento dell'azione delle funzioni di controllo interno.

BOX 4

Interazioni tra rischio informatico e rischi operativi (Capitolo8, Sezione II, par 1)

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

Il rischio informatico non è sistematicamente considerato nel suo complesso e valutato nelle BCC-CR.
Non sono sistematicamente disponibili politiche sul rischio informatico deliberate dal Consiglio di Amministrazione.
Ciò nonostante vengono svolte attività di valutazione tramite attività di Internal Auditing, basate sugli standard internazionali e le best practices di riferimento opportunamente adattati alla dimensione aziendale ed al grado di esternalizzazione dei sistemi informatici.

A livello di singola azienda, sono solo sporadicamente attivati sistemi di acquisizione di informazioni per la costruzione di serie storiche per la valutazione del contributo dei sistemi informatici sulla regolarità delle operazioni. L'implementazione di procedure di acquisizione di elementi che consentano la valutazione citata, su base quantitativa, appare difficile per una tradizionale poca attenzione al tema, salvo eccezioni.

Con riguardo all'approccio metodologico, si evidenzia che risulterebbe complesso ed oneroso, per le BCC-CR, supportare le valutazioni inerenti al rischio informatico per ogni ambito tecnologico con un approccio quantitativo; pertanto, si ritiene utile proporre l'adozione di approcci qualitativi in grado di supportare il processo decisionale in merito alle misure di mitigazione del rischio da adottare.

Ipotesi di sviluppo

Le BCC-CR dovrebbero:

a. definire le politiche in materia di sistemi informativi, specificando la "disponibilità al rischio".
   Si tratterebbe di:
   - deliberare il trasferimento dei rischi legati a sviluppo e continuità dei servizi all'outsourcer,
   - prendere atto della necessità di amministrare e valorizzare i servizi ottenuti in un quadro di conformità e sicurezza;
   - disciplinare i processi di valutazione/decisione/scelta e gestione della porzione di sistemi informativi non esternalizzata e le informazioni residenti sull'infrastruttura tecnologica interna;
b. tracciare linee guida per indirizzare comportamenti interni nel caso di inadeguatezza dei sistemi informatici e gestione del rischio emergente.

Ruolo delle strutture associative

Supportare le associate nello svolgimento delle attività di cui al punto a e b, sviluppando come d'abitudine uno o più modelli da personalizzare secondo le peculiarità della singola banca.

6. Organizzazione della funzione ICT. Figura del direttore dei sistemi informativi.

Q16 **Nella vostra istituzione esiste la figura del direttore dei sistemi informativi o figura equivalente?**

No.

Q17 **Quale sarebbe l'effetto sui costi dell'introduzione di tale figura?**

Presso le BCC-CR già esiste un soggetto con compiti di coordinamento organizzativo che includono la gestione degli aggiornamenti applicativi diffusi dall'outsourcer. La normativa d'altra parte, oltre al Direttore ICT (da sottoporre a considerazioni relative al principio di proporzionalità) introduce il c.d. "utente responsabile", identificabile come il *proprietario* di processi di business, con capacità di visione e responsabilità sugli applicativi informatici utilizzati nel proprio ambito.

Si prefigura quindi l'opportunità di definire formalmente una figura con compiti di coordinamento che si interpone tra gli utenti responsabili e l'outsourcer. Si tratta del "*Proprietario di contratto*" relativamente alle attività in outsourcing in generale e al caso informatico in particolare.
Occorrerebbe dunque sostenere costi particolarmente elevati.

Ipotesi di sviluppo

- definire le responsabilità del soggetto designato e individuare le linee guida per la reportistica utile ai fini del governo del rischio;
- chiarire il ruolo di "utente responsabile"
- strutturare un articolato di documenti come indirizzato nell'allegato A del documento in consultazione.

Ruolo delle strutture associative

- Definire il job profile del "*proprietario di contratto di esternalizzazione*" dettagliandone responsabilità, compiti e attività, contenuti e tempi della reportistica da produrre per i vertici aziendali;
- Idem per gli "utenti responsabili"

- sviluppare metodologie e strumenti a supporto dell'attività, con riferimento sia ai controlli sia alla reportistica;
- predisporre un piano di formazione sia per la nuova figura, sia per coloro che interagiscono con essa;
- fornire assistenza/consulenza nel tempo.

BOX 3

Declinazione del principio di proporzionalità (Capitolo 7, Sezione III, paragrafo1)

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.

Gli Enti di Categoria si avvalgono riguardo ai profili di complessità dimensionale di criteri basati su numero delle dipendenze, numero dei dipendenti, turn-over
Con riferimento alla complessità operativa si ritiene che vadano sviluppate considerazioni in merito alla rischiosità intrinseca a determinati prodotti/servizi, riconoscendo la diversa/minore complessità legata al mantenimento di profili operativi "tradizionali" e poco rischiosi.