Disposizioni di Vigilanza prudenziale per le Banche

Sistema dei Controlli Interni, Sistema Informativo e Continuità Operativa

RISPOSTA AL DOCUMENTO DI CONSULTAZIONE

novembre 2012

Contenuti

Premessa ed *Executive Summary*

Si ringrazia Banca d'Italia per aver dato la possibilità di formulare osservazioni, commenti e proposte sullo schema di Disposizioni di Vigilanza Prudenziale per le Banche in materia di sistema dei controlli interni, di sistema informativo delle banche e dei gruppi bancari, nonchè di continuità operativa delle banche e degli intermediari. Si ringrazia inoltre per la proroga accordataci che ha consentito di discutere i contenuti del presente documento di risposta anche con il Collegio Sindacale, il Comitato Controlli Interni e Rischi e alcuni esponenti aziendali.

Nel corpo del presente documento sono riportate le considerazioni generali, i principali punti di attenzione, i commenti agli specifici quesiti formulati negli appositi Box, nonché le osservazioni e le richieste di chiarimento relative al testo in consultazione.

Prima di entrare nel merito delle singole sezioni, UniCredit, anche in relazione alla propria articolazione dimensionale, ritiene indispensabile esprimere alcune osservazioni su taluni aspetti contenuti nelle Disposizioni in consultazione. Tale necessità emerge dall'impatto – non ultimo economico – che le "nuove" previsioni, così come formulate, potrebbero provocare, anche in termini di svantaggio competitivo delle banche più grandi verso quelle di minori dimensioni.
A tal riguardo segnaliamo all'Autorità la necessità di tenere conto anche della concorrenza degli operatori para-bancari o "non totalmente" bancari (specie nell'ambito dei pagamenti), ovvero delle banche di più piccole dimensioni, che, rispetto a quanto disposto, potrebbero essere soggette a previsioni normative o soluzioni organizzative meno vincolanti.

Di seguiti quindi gli argomenti di maggiore rilevanza.

1) **Con riferimento alle principali finalità** dello schema di disciplina, che vengono specificatamente indicate: (i) nel rafforzamento della capacità delle banche di gestire i rischi aziendali, e (ii) nella revisione organica dell'attuale quadro normativo, pur condividendo appieno i sopraccitati obiettivi si vuole evidenziare - per la prima finalità - che la scelta di entrare talora significativamente nel merito delle soluzioni organizzative delle aziende bancarie, sembra non tenere conto appieno sia delle diversità esistenti tra le banche del sistema italiano, sia del rilevante impatto economico di alcune di esse.

   Quanto alla seconda finalità, si suggerisce di valutare la razionalizzazione in ottica "testo unico" di un più ampio spettro di normative di vigilanza e regolamentari, anche al fine di ridurre i casi di possibile disallineamento o di parziale completezza. Il sistema bancario sente l'esigenza di avere un testo di riferimento chiaro e completo in quanto le possibili lacune o sovrapposizioni possono avere riflessi sull'efficacia del sistema dei controlli.

2) **Con riferimento al ruolo e alle responsabilità degli organi aziendali**, le nuove Disposizioni, oltre a fornire un quadro parziale delle responsabilità finali e dei flussi informativi, fanno confluire verso questi organi responsabilità gestionali talora non coerenti con la finalità prima e la forma collegiale degli stessi. L'impostazione scelta rischia così di:

   - snaturare il ruolo in particolare dell'organo con funzione di supervisione strategica.

     Nello specifico si fa riferimento al collocamento della funzione di controllo dei rischi (*risk management*) alle dirette dipendenze del citato organo. In tal modo infatti, verrebbe affiancato al suo riconosciuto compito di definizione delle strategie industriali e dell'appetito/tolleranza ai diversi rischi, anche quello di monitoraggio nel continuo degli stessi.

     Tale soluzione organizzativa, che sposta il "*check and balance* quotidiano" verso il consiglio di amministrazione, avrebbe un impatto rilevante sia sul numero delle sedute dell'organo sia sulla presenza di competenze specifiche da parte dei suoi membri, sia soprattutto sulla tempestività, sulla laboriosità e quindi sull'efficacia del processo decisionale. Ancor meno praticabile appare l'ipotesi di diretto riporto della funzione *risk management* al comitato

controllo e rischi, in quanto alle considerazioni sopra esposte, si aggiunge quella della natura consultiva dello stesso.

Inoltre soluzioni che assegnano attività di gestione quotidiana dei controlli sui rischi all'organo con funzione di supervisione strategica – deputato alla definizione del corretto bilanciamento fra rischi e rendimento e alla supervisione del suo rispetto – incidono sulle leve di controllo diretto del management con possibili riflessi sulla sua "*accountability*".

- assegnare univocamente all'organo con funzione di gestione attività operative dirette.

  Si cita come esempio più rilevante l'attribuzione del "*regolare funzionamento dei sistemi informativi*". Si ritiene che in realtà bancarie con articolazione dimensionale quale quella di UniCredit, responsabilità di questa importanza debbano poter essere assegnate a figure di vertice quali, come nel nostro caso al *Chief Operating Officer,* comunque a diretto riporto dell'amministratore delegato. Tale soluzione consente peraltro anche un maggiore coordinamento con la funzione di Organizzazione.

Si suggerisce dunque di:

- rappresentare gli organi aziendali e le funzioni in un quadro olistico che consenta una visione a 360° in termini di ruoli, interazioni e flussi informativi,
- articolare gli organi aziendali in maniera tale da garantire un efficace bilanciamento tra supervisione e gestione d'azienda, prevedendo la discrezionalità per le banche di mantenere la funzione di controllo dei rischi a riporto della figura di vertice deputata a condurre la gestione aziendale, al fine di assicurare alla stessa tutte le leve necessarie anche a esercitare il controllo dell'attività aziendale,
- prevedere soluzioni organizzative che assicurino "accesso diretto" dei responsabili della funzione agli organi aziendali, definendo altresì flussi informativi completi e organici a garanzia del ruolo di supervisione degli organi stessi.

3) Con riferimento alle funzioni di controllo in generale siamo convinti che il rafforzamento del sistema dei controlli passi attraverso una maggiore informativa, chiara e trasparente, e non necessariamente attraverso un ulteriore distacco gerarchico-organizzativo delle funzioni di Business da quelle di controllo.

Riteniamo che la crescente tendenza a trattare dette funzioni in maniera separata e indipendente - fuori da una visione integrata - unita all'enfasi data ai controllo sui rischi e sulla conformità (cd. "secondo livello"), possano ingenerare un potente effetto non voluto di accentuazione della logica "a silos", contribuendo in qualche modo a deresponsabilizzare il Business, primo responsabile del processo di gestione dei rischi stessi.

Dal punto del posizionamento organizzativo, infine, fermo restando quanto sopra, qualora venisse attuato quanto previsto nel Documento di consultazione, non risulterebbe chiaro perché una sola funzione di controllo di secondo livello dovrebbe riportare all'organo con funzione di supervisione strategica - al quale peraltro riporta quello di terzo livello dell'Internal Audit – mantenendo così la sola funzione di conformità alle norme a riporto dell'organo con funzione di gestione.

Anche per questo ambito il suggerimento passa attraverso una rappresentazione organica delle attività di controllo e dei relativi flussi informativi da indirizzare obbligatoriamente e a tutti i livelli aziendali. Vengono infatti indicati i flussi da indirizzare alle strutture e agli organi di vertice, a nostro avviso trascurando l'importanza che rivestono tali flussi anche per le strutture di Business. Una rappresentazione in tal senso contribuirebbe a garantire l'effettivo esercizio di supervisione di ciascun livello aziendale rispetto alla responsabilità ricoperta.

4) Con riferimento alla funzione di conformità si ritiene difficilmente applicabile l'allargamento del perimetro di responsabilità di detta funzione alla gestione del rischio di non conformità alle norme per tutta l'attività aziendale e con particolare attenzione alla normativa fiscale (peraltro

inclusi i rischi derivanti dal coinvolgimento in operazioni fiscalmente irregolari poste in essere dalla clientela). Oltre infatti agli ingenti costi connessi - riferibili sia alla numerosità sia al livello professionale delle risorse necessarie - si rischia di formalizzare un ruolo indefinito della funzione di conformità, anziché consentirne la maggiore focalizzazione sulle normative prettamente bancarie e finanziarie, incidendo così sull'identità della funzione stessa.

Considerata la sua attività maggiormente trasversale rispetto alla funzione di controllo dei rischi (*risk management*), per la funzione di conformità si suggerisce che le Disposizioni forniscano non solo l'ambito di presidio normativo, i principali adempimenti e le aree di intervento, ma anche ne descrivano chiaramente la natura e il ruolo che la Vigilanza si attende da questa funzione, in particolare sull'attività ex-ante e sui controlli ex-post, questi ultimi specie nel continuo.

5) **Con riferimento ai tempi di implementazione**, considerati tutti gli elementi con impatti significativi sull'organizzazione aziendale sia in termini di numerosità sia in termini di tempi di "messa a punto", si chiede che vengano comunque valutati tempi idonei di implementazione delle nuove previsioni, anche con riferimento al quadro normativo complessivo, sia italiano sia estero.

In ogni caso, considerata l'articolazione del sistema bancario italiano si suggerisce di prevedere da parte dell'Autorità di Vigilanza, una procedura di valutazione delle diverse soluzioni organizzative che - nel pieno rispetto dei principi alla base di una sana e prudente gestione delle Banche, della salvaguardia della stabilità del sistema finanziario e di un efficace funzionamento del sistema dei controlli interni - dovessero presentare differenze di modello dettate da specifiche esigenze, non ultime quelle dimensionali.

In conclusione, e fermo restando quanto detto sopra e nel testo della presente risposta, si richiamano di seguito i tre ambiti che, a parere di UniCredit, codesta Autorità dovrebbe tenere maggiormente in considerazione nel testo definitivo delle Disposizioni: (i) l'esigenza che le "nuove" Disposizioni vengano formulate quanto più possibile in ottica di "testo unico"; (ii) l'esplicitazione di chiare linee guida nei vari ambiti di presidio dei rischi, lasciando però maggiore spazio di autonomia alle singole banche nella definizione delle diverse soluzioni organizzative, anche in ottica di piena attribuzione delle responsabilità e delle relative leve al management (ci riferiamo ad esempio al riporto del *risk management*), e (iii) la definizione completa, integrata e organica dei flussi informativi delle diverse funzioni di controllo e i loro destinatari.

Principali punti di attenzione

In questo paragrafo sono riassunti i punti che UniCredit ritiene di maggiore rilievo e per i quali vengono riportate le osservazioni di dettaglio nelle altre sezioni del presente documento di risposta.

- **Organi aziendali**

  Si suggerisce di esplicitare con maggiore chiarezza i differenti livelli di valutazione delle diverse materie assegnate a ciascun organo aziendale. A puro titolo esemplificativo l'organo con funzione di supervisione strategica (ma analoga considerazione può essere fatta per quello di gestione) talora "*definisce*", talora "*approva*", talora "*assicura*", alcune volte "*valuta*" oppure "*individua*" ovvero "*esamina*" le diverse materie di competenza. La terminologia usata infatti non garantisce una univoca comprensione del livello approvativo e di responsabilità finale dell'organo, nonché della profondità richiesta dalla materia di volta in volta presa in considerazione. In particolare nei casi in cui gli organi sono chiamati a "*individuare*", non sempre si riscontra presso gli altri organi o funzioni aziendali l'espresso riferimento a chi debba farsi carico di proporle. Sempre a titolo esemplificativo non pare marginale, in ottica di revisione organica della normativa, il fatto che le responsabilità in capo agli organi aziendali in materia ICT siano declinati nella sola Sezione II del Capitolo 8 sul Sistema Informativo, anziché essere riportati in maniera esaustiva anche nella Sezione II - Il ruolo degli organi aziendali, del Capitolo 7 - Il sistema dei controlli interni.

- **Posizionamento organizzativo della funzione di controllo dei rischi** (*risk management function*)

  Emerge dalla lettura del testo in consultazione che la previsione del possibile collocamento del solo responsabile della funzione di controllo dei rischi "*alle dirette dipendenze del comitato controllo e rischi, ove costituito, o dell'organo con funzione di supervisione strategica*" al fine di rafforzarne l'indipendenza, si restringe poi a un obbligo per le Banche classificate nelle macro-categorie 1 e 2 a fini SREP, di collocare l'intera funzione di controllo dei rischi alle dirette dipendenze degli stessi organi.
  Al di là della disparità tra banche di diverse dimensioni, ci sembra che nel tentativo di tutelare il legittimo principio di accesso diretto dei responsabili delle funzioni di controllo agli organi aziendali di vertice – espresso nella Sezione III del Capitolo 7 e a nostro avviso attivabile attraverso altri meccanismi organizzativi - si stia imponendo una soluzione organizzativa gestionale onerosa per gli organi aziendali che di fatto sottrae all'amministratore delegato una componente fondamentale di controllo diretto e dei relativi flussi informativi tempestivi.
  Considerata infatti la natura gestionale delle attività in capo alla funzione di controllo dei rischi definita nel testo come funzione deputata ad "*attuare le politiche di governo dei rischi, attraverso un adeguato processo di gestione dei rischi*", ci si domanda quali dovrebbero essere le modalità di conduzione della funzione nel continuo in caso la stessa dipendesse dall'organo con funzione di supervisione strategica, rispetto ad esempio alle priorità della gestione corrente. Difficile pensare che la conduzione possa risultare più attuabile se la funzione di *risk management* fosse posta a riporto del comitato controllo e rischi, anche con riferimento alla sua natura consultiva.
  Per completezza di valutazione, anche volendo accettare la posizione espressa dal Documento in consultazione, resta non del tutto chiaro il razionale del diverso posizionamento che la funzione di conformità alle norme avrebbe rispetto a quella di controllo dei rischi.

- **Perimetro di responsabilità della funzione di conformità alle norme** (*compliance function*)

  Il testo della consultazione, dopo aver richiamato in via generale le norme più rilevanti ai fini del rischio di non conformità, specifica che "*tuttavia, la funzione presiede alla gestione del rischio di non conformità alle norme, con riguardo a tutta l'attività aziendale*". Così declinata

la previsione pare di difficile e onerosa attuazione in quanto porterebbe significativi impatti in termini di:

- efficacia, per l'ampia dispersione rispetto all'importanza che riveste il presidio attento della funzione sulle norme che tutelano il consumatore e alcuni aspetti patrimoniali (ad esempio ci si domanda se rientrerebbero nel novero alcune normative certamente importanti, ma non direttamente attinenti alla attività bancaria o finanziaria come quella sulla sicurezza sul lavoro),
- assetto organizzativo, per la possibile confusione e/o sovrapposizione dei ruoli nella definizione dei processi aziendali e nell'attività di controllo degli stessi,
- efficienza, per l'allargamento e/o duplicazione delle competenze specialistiche.

Si chiede dunque di focalizzarne le attività, descrivendone le finalità ex-ante e i controlli ex-post, questi ultimi specie nel continuo.
Inoltre, pur condividendo appieno la necessità di un presidio efficace della conformità dell'attività aziendale alle normative di natura fiscale, si esprimono perplessità sulla sua attribuzione alla funzione di conformità alle norme, sia richiamando gli elementi di carattere generale sopra menzionati, sia chiedendo chiarimenti sulla effettiva applicazione di una simile previsione, in particolare in relazione ai "*rischi derivanti dal coinvolgimento in operazioni fiscalmente irregolari poste in essere dalla clientela*".
Si suggerisce comunque di attendere l'esito dell'esame del disegno di legge delega in materia, da parte del Parlamento.

- **Funzioni e livelli di controllo**

UniCredit concorda con la nuova previsione contenuta nel Documento per la consultazione (e non presente nelle Disposizioni di Vigilanza in materia di conformità del Luglio 2007), che stabilisce che "*l'attività di prevenzione deve svolgersi in primo luogo dove il rischio viene generato: è pertanto necessaria un'adeguata responsabilizzazione di tutto il personale*". Di fatti, la funzione di compliance presidia il rischio di non conformità svolgendo le attività descritte nel Documento di consultazione, supportando la banca e le sue strutture operative, ma è evidente che la prevenzione e la gestione del rischio devono essere una responsabilità prima di tutto in capo alle funzioni operative. Su questo aspetto suggeriamo di sviluppare, nel quadro del sistema dei controlli interni nel suo complesso, in maniera più estesa la tematica dei controlli di primo livello attribuiti alle funzioni operative, integrando quanto previsto a pagina 5 del paragrafo 6 - Principi generali. In particolare si suggerisce di articolare maggiormente i paragrafi relativi ai controlli di primo e secondo livello (in particolare su quest'ultimo viene solo esplicitato che gli stessi "*hanno l'obiettivo di assicurare, tra l'altro: […]*", non fornendo quindi una indicazione esaustiva della loro finalità). Si riterrebbe utile anche una maggiore sistematicità e organicità nella elencazione e descrizione dei flussi informativi e soprattutto delle relazioni periodiche in carico alle diverse funzioni di controllo, inclusa quella di revisione interna. Non risulta sempre uniforme infatti l'iter di validazione dei diversi documenti da sottoporre successivamente all'"*esame*" dell'organo con funzione di supervisione strategica.

- **Responsabili delle funzioni di controllo**

Tra gli altri temi più di dettaglio, per i quali si rimanda alle pagine seguenti, si evidenzia qui la necessità di ricevere chiarimenti su:

- l'esatta declinazione della previsione circa l'impossibilità che i responsabili delle funzioni di controllo abbiano responsabilità "*diretta*" di aree operative sottoposte a controllo,
- l'organo effettivamente deputato alla nomina e revoca dei responsabili delle funzioni di controllo in quanto il Documento di consultazione dispone che essi "*siano nominati e revocati (motivandone le ragioni) dall'organo con funzione di gestione, d'accordo con l'organo con funzione di supervisione strategica, sentito l'organo con*

funzione di controllo", diversamente da quanto previsto nell'ambito delle Disposizioni sul Governo Societario (Banca d'Italia, 4 marzo 2008) secondo cui "*la nomina del responsabile delle Funzioni di revisione interna e di conformità rientra tra le attribuzioni non delegabili del Consiglio di Amministrazione*".

- **Organo con funzione di controllo e D. Lgs. 321/01**

  Con riferimento alla previsione che assegna all'organo con funzione di controllo le funzioni dell'organismo di vigilanza, non risulta di immediata comprensione quali possano essere le "*particolari e motivate esigenze*" per poter affidare tali funzioni a un organismo appositamente istituito.

- **Esternalizzazione di funzioni aziendali**

  Nel rimandare alle osservazioni di dettaglio formulate nelle pagine seguenti, si vogliono qui sottolineare gli aspetti considerati maggiormente critici per realtà dimensionalmente articolate come quella di UniCredit. In particolare:

  - ferma restando la capacità di controllo e la responsabilità sulle attività esternalizzate, si chiede di differenziare il caso di esternalizzazione infragruppo (incluso il riferimento all'informativa preventiva da fornire a Banca d'Italia) da quello di esternalizzazione a terzi al fine di garantire un adeguato livello di presidio anche in termini di efficienza economica,
  - la previsione di mantenimento delle "*competenze tecniche e gestionali essenziali per re-internalizzare, in caso di necessità*" lo svolgimento delle attività esternalizzate, così come formulata, sembra difficilmente applicabile, soprattutto - ma non solo - nel caso di attività non core o non di controllo esternalizzate verso terzi,
  - la previsione di un "*referente per le attività esternalizzate*" se inteso come unico punto di sintesi non risulta attuabile, anche con riferimento alla sua allocazione organizzativa.

- **Posizionamento organizzativo della funzione e del responsabile ICT**

  Non pare facilmente applicabile in realtà dimensionalmente articolate come quella di UniCredit, che l'organo con funzione di gestione sia il referente primo dell'efficacia e del regolare funzionamento dei sistemi informativi e che lo stesso possa, ad esempio, disegnare e seguire "*l'implementazione dei processi di gestione dell'ICT […]*". La normativa dovrebbe prevedere, a parità di responsabilità, allocazioni organizzative differenziate.

  Riteniamo di formulare analoga osservazione per "*la linea di riporto diretta verso l'organo con funzione di gestione*" prevista dal testo di consultazione per il "*Direttore dei sistemi informativi*".

- **Procedura di Allerta Interna**

  Pur condividendo appieno il razionale alla base di una simile procedura, si suggerisce di valutare con attenzione l'attuale formulazione inserita nel Documento di consultazione in quanto non ci si limiterebbe a dover gestire tutte le segnalazioni volte a evidenziare possibili "*irregolarità nella gestione della banca o violazioni delle norme disciplinanti l'attività bancaria*", ma anche tutte le segnalazioni di "*eventuali disfunzioni dell'assetto organizzativo o del sistema dei controlli interni"*. Considerata l'onerosità di una simile procedura si suggerisce, in linea con la prassi a livello internazionale in tema di *Whistleblowing*, di privilegiare l'approccio più restrittivo dei casi di possibile illiceità, violazione di norme o non conformità, lasciando le segnalazioni relative a disfunzioni organizzative o del sistema dei controlli interni alle procedure ordinarie degli intermediari.

Risposte ai Box

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

Box 1

La tolleranza al rischio (*risk tolerance*) e l'appetito per il rischio (*risk appetite*) sono entrambi utilizzati per descrivere sia il livello assoluto di rischio che una banca è a priori disposta ad assumere, sia i limiti effettivi che essa pone nell'ambito di tale livello massimo. Al fine di valutare l'opportunità di individuare parametri utilizzabili per determinare il livello di rischio assumibile si sollecita l'indicazione delle variabili quantitative e qualitative correntemente utilizzate o in via di sviluppo per addivenire a tale determinazione

Nel Gruppo UniCredit, il risk appetite è definito in termini di identificazione delle metriche, dei relativi target (valori obiettivo), trigger (valori di allerta) e limiti (valori da non superare) dal Comitato Rischi di capogruppo a seguito di una proposta congiunta da parte delle funzioni competenti di Planning Finance & Administration (PFA) e Group Risk Management (GRM) e in accordo con le tempistiche del processo di budgeting (breve e medio termine). Il risk appetite è approvato dal consiglio diaAmministrazione della capogruppo e inviato alle società del Gruppo per la loro applicazione ed eventuale calibrazione locale, ove richiesta da requisiti dell'Autorità di Vigilanza locale, secondo le scadenze dei processi di pianificazione.

Attualmente le metriche utilizzate nel Gruppo UniCredit sono raggruppate in tre dimensioni (Adeguatezza del Capitale, Redditività & Rischio, Liquidità &Funding), che insieme compongono il quadro di riferimento del risk appetite.

Dette metriche di adeguatezza patrimoniale, due (Core Tier 1 Ratio e Total Capital Ratio) garantiscono il bilanciamento tra capitale disponibile e profilo di rischio, misurato secondo quanto disposto dal Primo Pilastro di Basilea 2; una (Leverage Ratio) ha lo scopo di garantire la coerenza tra le dimensioni del capitale proprio e degli attivi in bilancio e una (RiskTakingCapacity, ovvero il rapporto tra Risorse Finanziarie Disponibili e Capitale Interno), definita in coerenza con il quadro di riferimento interno di Secondo Pilastro, fornisce un'indicazione della capacità economica di assunzione dei rischi da parte del Gruppo.

La metrica di Redditività & Rischio (LossAbsorptionCapacity) definisce quanto il Gruppo possa permettersi di perdere in termini di Conto Economico sulla base dei rischi assunti e guida il budget attraverso la definizione dei limiti.

Tra le metriche di Liquidità &Funding, il Cash Horizon, lo Structural Ratio e il SurvivalPeriod dello Stress Test della liquidità sono definiti in coerenza con la Liquidity Policy del Gruppo, mentre il Loan-Depo Gap è funzionale all'obiettivo del Gruppo di ottimizzare struttura e costi del funding.

La presenza di "Piani di Continuità Operativa" influisce sul calcolo delle componenti di alcune metriche del risk appetite. Infatti con riferimento alla componente di assorbimento di capitale da "rischio operativo" (Primo Pilastro – Advanced Measurement Approach - AMA) la presenza dei piani di continuità produce due effetti:

a. Un effetto indiretto sul livello di perdite operative dovuto alla mitigazione che di fatto avviene ogni qual volta, a fronte di incidenti anche non gravi, viene attivata la soluzione di continuità operativa al fine di garantire il 100% del servizio (realmente avvenuto più volte)

b. Un effetto diretto nell'ambito delle "Analisi di scenario" dove per alcuni event type (5-"Damages to physical assets" e 6-"Business disruption and system failures"), viene specificatamente dichiarato come i piani di *Business Continuity* siano fonte di mitigazione ed in alcuni casi incidano direttamente sul dato "maximum expected loss".

A seguito della definizione di metriche e di target/trigger/limiti, il risk appetite viene regolarmente monitorato e un processo di escalation ai livelli organizzativi appropriati garantisce una reazione tempestiva nel caso in cui i valori delle metriche si avvicinino o superino trigger e limiti.

La definizione di strategie/policy di rischio rappresenta un passaggio chiave dell'integrazione del risk appetite nel business ed è il modo con cui Group Risk Management comunica e incorpora target e limiti delle esposizioni di rischio nelle attività del Gruppo.

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

Box 2

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

Per quanto riguarda la definizione di criteri in base ai quali individuare le operazioni di maggior rilievo da sottoporre al vaglio preventivo della funzione di controllo dei rischi, richiamiamo le disposizioni in materia di "*Attività di rischio e conflitti di interesse nei confronti di soggetti collegati*" che - sebbene focalizzate sul presidio dei rischi nei confronti di quei soggetti che potrebbero influire sulle decisioni adottate dalla banca(soggetti collegati) - potrebbero fornire validi spunti – ferma la loro applicazione ad una categoria più estesa - per l'individuazione dei parametri in base ai quali identificare le operazioni di maggiore rilevanza, essendo un concetto già contemplato dalla predetta normativa[1]. In tal modo, si eviterebbero problemi di coordinamento tra le richiamate disposizioni, entrambe volte a presidiare il contenimento del rischio nelle sue diverse configurazioni.

Si sottolinea, peraltro, che per i gruppi bancari di una certa dimensione, dotati di patrimonio di vigilanza elevato in valore assoluto, il 5% dello stesso rappresenta una esposizione al rischio così alta da far sì che le operazioni che rientrano in questa fattispecie siano in numero esiguo. Si ritiene quindi che, in questi casi, l'adozione di una soglia più bassa (magari il 2% del patrimonio di vigilanza, come suggerito nel Titolo V – Capitolo, nell'ambito delle disposizioni sulle procedure per l'assunzione dei grandi rischi con riferimento alla valutazione dei legami di connessione tra i clienti) possa più efficacemente consentire alla funzione di controllo dei rischi di garantire la coerenza delle decisioni di maggior rilievo con la politica di governo dei rischi stabilita dalla banca e/o dal Gruppo.

1 Si riporta per pronto riferimento la definizione di operazione di maggiore rilevanza contemplata in materia dalle "Nuove Disposizioni di Vigilanza Prudenziale per le Banche": "*l'operazione con soggetti collegati il cui controvalore in rapporto al patrimonio di vigilanza (consolidato, nel caso di gruppi) è superiore alla soglia del 5% calcolata secondo quanto riportato in allegato, alla voce "Indice di rilevanza del controvalore". Per le operazioni di acquisizione, fusione e scissione la soglia, sempre del 5%, va calcolata secondo le modalità indicate in allegato alla voce "Indice di rilevanza dell'attivo". La banca può individuare altre operazioni da considerare di maggiore rilevanza in base a indicatori qualitativi o quantitativi. In caso di operazioni tra loro omogenee o realizzate in esecuzione di un disegno unitario, compiute, nel corso dell'esercizio, con uno stesso soggetto collegato, la banca cumula il loro valore ai fini del calcolo della soglia di rilevanza*"

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

Box 3

La bozza di disciplina, in linea con il principio di proporzionalità, consente alle banche di accorpare ovvero esternalizzare le funzioni di controllo.

Si sollecitano commenti per declinare nel concreto tale principio, sulla base di criteri riferiti alla dimensione e alla complessità operativa delle banche nonché avuto riguardo all'esigenza di assicurare un rapporto ottimale costi/benefici nell'articolazione e nella conduzione dei controlli.

UniCredit ritiene che un approccio rigidamente quantitativo nell'applicazione del principio di proporzionalità in relazione all'esternalizzazione delle funzioni di controllo, comporti eccessive limitazioni alle scelte organizzative della banca.

Premesso quanto sopra, con riferimento alla declinazione nel concreto del principio, tra i criteri per determinare la complessità dimensionale si potrebbero annoverare, ad esempio, criteri di carattere quantitativo riferiti all'Attività svolta ed alla Dimensione Entità; in particolare:

per le Attività

- Servizi e Prodotti (tipologia e numero di attività bancarie, finanziarie e strumentali
- svolte);
- Clienti e controparti (tipologia e ubicazione dei clienti);
- Canali di Marketing (tipologie di canali di vendita e promozionali utilizzati dalla Entità);
- Governance e leggi locali (struttura proprietaria, accordi di esternalizzazione e requisiti delle normative locali.

per la Dimensione

- Patrimonio;
- Ricavi;
- FTEs;
- Numero di Controllate dirette e indirette;
- Numero di clienti per tipologia.

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

Box 4

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

Per quanto riguarda l'integrazione del rischio informatico nella definizione dell'appetito al rischio, che riteniamo peraltro estremamente sfidante, il Gruppo UniCredit già prevede degli strumenti similarmente alle altre categorie di rischio rientranti nella definizione di rischio operativo. Ad oggi infatti nella definizione della Loss Absorption Capacity (LAC) del Gruppo vengono già inserite le perdite a conto economico stimate per i rischi operativi, incluse quelle dovute al rischio informatico, così come sono incluse le "misure interne" di Capitale Economico a fronte dei rischi operativi nella Risk Taking Capacity. Ulteriori passi per inserire più esplicitamente la variabile di rischio informatico dentro il framework di risk appetite, richiedono tempi di implementazione non irrilevanti sia per l'individuazione delle metriche corrette sia per la loro condivisione e tracciabilità.

Relativamente alle modalità di integrazione/interazione tra il governo della variabile informatica e la gestione dei rischi operativi, si suggerisce l'adozione di modelli e schemi standard/tipici della practice di Risk Management ed in vigore per altri rischi aziendali. In particolare:

- lo sviluppo della modellistica/metodologia di analisi del rischio, in capo alla funzione indipendente del Risk Management,
- la definizione delle azioni di contenimento/riduzione dei rischi , in capo alla funzione ICT,
- l'approvazione della metodologia e dei piani formali di azione, da parte dell'organo di gestione.

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

Box 5

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

Per quanto attiene alla richiesta di commenti sui sistemi in Cloud Computing, in caso di outsourcing a terze parti e in modo specifico nel cloud computing di tipo pubblico, riportiamo di seguito le nostre considerazioni.

Concordiamo con l'opinione che i modelli attuali di Cloud ereditino le vulnerabilità e le minacce delle tecnologie su cui esse si fondano, amplificandole in termini di scala, ed esponendo maggiormente le aziende in termini di data integrity e di internet vulnerabilità.

L'utilizzo di risorse condivise e la non sempre facile identificazione dell'ubicazione territoriale rende più complicato il controllo di come i dati sono gestiti (in termini di CRUD) ed in termini dei dispositivi di sicurezza minimi da utilizzare.

La tecnologia Cloud richiede di analizzare approfonditamente il modello di servizio del provider e quali architetture e soluzioni egli utilizzi. Va in altre parole stabilito il concetto di "trasparenza" in opposizione al classico modello "*black-box*" dove il provider fornisce un servizio senza esplicitare e condividere le modalità attraverso cui lo eroga. In tal senso, per esempio, risulta fondamentale analizzare e verificare le "dipendenze" delle applicazioni rispetto ai servizi erogati e al modo con il quale questi servizi sono interconnessi a livello di flussi di dati. Altro aspetto rilevante e' la gestione della Business Continuity e della sicurezza dei dati (Integrity, Backup etc).

Suggeriamo l'utilizzo di approcci di Virtual Data Center, segregando per servizi di business all'interno di una unità logica, anziché segregare per tecnologia, in modo da limitare l'effetto domino in caso di malfunzionamenti e di aumentare la sicurezza e la possibilità di controllo.

Il provider dovrebbe fornire dati "grezzi" sulle prestazioni e consentire l'accesso ai log delle operazioni di base, abilitando il cliente ad un livello minimo di tracciabilità e alla possibilità di effettuare audit tecnici su quando accade nelle soluzioni.

Allo stesso modo il cliente dovrebbe essere abilitato all'accesso in lettura, alle configurazioni delle soluzioni.

Il provider dovrebbe fornire l'elenco delle localizzazioni dei diversi componenti e di come questi contribuiscono all'erogazione del servizio; allo stesso modo dovrebbe essere data visibilità di come viene realizzata la ridondanza, ove prevista.

Il cliente di soluzioni cloud deve essere interpellato nel caso in cui i dati e le soluzioni tecniche debbano essere spostare al di fuori di un determinato Paese. Questo per le ovvie implicazioni legali del trattamento dei dati stessi.

Sarebbe auspicabile che l'Autorità di Vigilanza definisca i controlli minimi che un intermediario debba poter effettuare su un provider Cloud in termini di configurazioni, sicurezza ed integrità dei dati. Riteniamo utile sottolineare i seguenti elementi, solo a titolo di esempio: log degli accessi, SLA, test di DR/BCM, interoperabilità visibilità sui change ad impatto rilevante, crittografia e livelli di sicurezza, antivirus, visibilità degli incidenti di disponibilità e piani correttivi (incident management/problem management).

Commenti particolari

TITOLO V – CAPITOLO 7 - IL SISTEMA DEI CONTROLLI INTERNI

SEZIONE I - DISPOSIZIONI PRELIMINARI E PRINCIPI DI CARATTERE GENERALE

1.1 Premessa

Nulla da osservare

1.2 Fonti normative

Nulla da osservare

1.3 Definizioni

In via generale, appare opportuno sottolineare che nel Documento di consultazione si riscontrano delle indicazioni (ad esempio "*funzioni aziendali e societarie di controllo*") che non appaiono ricomprese nel perimetro delle "Definizioni". Si suggerisce, pertanto, al fine di evitare fraintendimenti, di allineare tutte le suddette indicazioni al perimetro delle "Definizioni". Nello stesso senso, si ritiene opportuno adottare il medesimo approccio per l'utilizzo di espressioni simili, ma che possono comportare delle letture differenti ("*esamina/valuta*", "*definisce/approva*", "*sottopone/propone*",…).

Con specifico riferimento alla nozione di "*funzioni aziendali di controllo*", si rileva un disallineamento con il Documento "The internal audit function in banks", principio 13, laddove include tra le "*second line of defence*" anche human resources, technology, legal, finance, operations, oltre alle ben note risk management e compliance. Si richiede, in proposito, una precisazione circa gli ambiti delle funzioni aziendali di controllo.

1.4 Destinatari della disciplina

Nulla da osservare

1.5 Unità organizzative responsabili dei procedimenti amministrativi

Nulla da osservare

1.6 Principi generali

Con riguardo alla mission della revisione interna, vengono introdotti i concetti di "*completezza*" e "*adeguatezza*" in termini di efficienza ed efficacia, il che potrebbe trattarsi solo di una più dettagliata ed ampia descrizione del concetto già in precedenza espresso nella Circolare 229 ("…*funzionalità del complessivo sistema dei controlli interni*"). Premesso che l'Internal Audit può assicurare la completezza limitatamente alle attività svolte nell'ambito del piano di audit, si richiede di chiarire il concetto di "completezza".

Si rileva, infine, che la dicitura "*le banche*" appare troppo generica per stabilire a quale organo aziendale deve essere affidato il compito di controllare il grado di aderenza ai requisiti del sistema dei controlli interni e dell'organizzazione e adottare le misure adeguate ("*verificano regolarmente, con frequenza almeno annuale, il grado di aderenza ai requisiti del sistema dei controlli interni e dell'organizzazione e adottano le misure adeguate per rimediare a eventuali carenze*"). Appare, pertanto, necessaria una precisazione in merito a quale organo aziendale debba essere demandato tale compito e se tale verifica rientri nelle relazioni annuali di competenza delle funzioni di controllo.

SEZIONE II - IL RUOLO DEGLI ORGANI AZIENDALI

1.1 Premessa

Circa il ruolo degli organi aziendali, con specifico riferimento alle responsabilità relative al sistema dei controlli interni, si suggerisce di introdurre delle indicazioni sintetiche da cui sia possibile evincere le singole responsabilità di ciascuno di essi. Un quadro sinottico potrebbe fungere da valido supporto, con indicazione dell'organo cui è attribuita la specifica attività, caratterizzata per tipologia (ad esempio mediante le indicazioni "*valutazione*", "*verifica*", "*attuazione*"). E' comunque opportuno, a nostro avviso, che venga data anche una chiara definizione delle azioni di "*valutazione*", "*verifica*", "*attuazione*" anche al fine di garantire un corretto esercizio della responsabilità.

Da ultimo, quale rilievo generale, si evidenzia come – data la scelta effettuata di procedere a una definizione analitica delle competenze, responsabilità, profili e contenuti dei vari ambiti (organi aziendali, funzioni, rapporti tra essi,..) oggetto di analisi nel Documento di consultazione – appaia più che necessaria un'attenta rilettura delle singole Sezioni e delle relazioni tra di esse a evitare, come si riscontra in alcuni passaggi attuali del Documento di consultazione, situazioni di mancanza di coordinamento o di veri e propri "vuoti" di disciplina.

1.2 Organo con funzione di supervisione strategica

Con riferimento, nello specifico, al par. 2, secondo alinea lett. c), dopo aver indicato che è compito dell'organo con supervisione strategica definire "*i criteri per individuare le operazioni di maggior rilievo da sottoporre al vaglio preventivo della funzione di controllo dei rischi*" , (con un riferimento alla Sez. III par. 3.3. ove viene chiaramente delineato ciò che tale funzione è chiamata a fare), si aggiunge che (l'organo con funzione di supervisione strategica) deve indicare "*l'estensione, i limiti e le modalità di esercizio dei poteri di detta funzione*". Quest'ultimo periodo sembrerebbe una ripetizione rispetto alla previsione, più generale, contenuta al successivo terzo alinea, lett. a) relativa alla costituzione, attribuzioni e responsabilità delle funzioni di controllo. Se invece detto ultimo periodo va riferito solo alle operazioni di maggior rilievo sembrerebbe, anche in questo caso una ripetizione con quanto previsto nella Sez. II, par. 3, primo alinea lett. d) che individua chiaramente l'estensione dei poteri (emissione di parere) e i limiti (non vincolatività del parere) della funzione di controllo dei rischi per tale fattispecie. Nel dubbio, si chiede di chiarire il significato e la portata del secondo periodo del par. 2, secondo alinea, lett. c).

Passando, poi, a esaminare le altre competenze attribuite all'organo con funzione di supervisione strategica, la formulazione proposta riguardo alla già citata lett. a) del terzo alinea in merito alla costituzione delle funzioni aziendali di controllo risulta alquanto generica e ampia - soprattutto se riferita ad assetti organizzativi complessi e strutturati - e potrebbe portare l'organo con funzione di supervisione strategica a occuparsi sin nella loro granularità di assetti organizzativi, aspetto che, si ritiene, possa invece tranquillamente rientrare nelle competenze dell'organo con funzione di gestione. Si propone, conseguentemente, di attribuire la competenza deliberativa in capo all'organo con funzione di supervisione strategica esclusivamente con riguardo alle strutture di primo livello che fanno capo ai responsabili delle funzioni di controllo.

In merito poi all'approvazione del processo per lo sviluppo e la convalida dei sistemi interni di misurazione dei rischi non utilizzati a fini regolamentari e alla verifica periodica del corretto funzionamento, pur riconoscendo la rilevanza di un presidio efficace anche sui modelli gestionali non riconosciuti ai fini regolamentari, sottolineiamo la necessità che vengano precisati i contenuti minimi di tali controlli. E' infatti difficilmente ipotizzabile che i sistemi gestionali vengano sottoposti a un processo di convalida analogo a quelli regolamentari, la cui verifica è già estremamente onerosa. Il processo in questione per essere sostenibile dovrà comunque essere configurato come particolarmente snello ed essenziale.

Inoltre si evidenzia che il coinvolgimento dell'organo con funzione di supervisione strategica dovrebbe qualificarsi più propriamente come "*approvazione*", Sez. II, par. 2, sesto alinea, (anziché come "*esame*")"*del programma di attività [omissis] predisposti dalle funzioni aziendali di controllo*

compreso il piano di audit predisposto dalla funzione di revisione interna". Quanto precede, peraltro, è in linea con le competenze demandate a predetto organo dal Codice di Autodisciplina, nonché dal Documento BCBS "The internal audit function in banks"; in particolare per quanto concerne la pianificazione delle attività della revisione interna, nonché al Regolamento Congiunto CONSOB-Banca d'Italia dell'ottobre 2007, anche per la funzione di conformità.

Potrebbe altresì essere opportuno sottolineare con maggiore evidenza a quale organo è attribuita la valutazione finale del sistema dei controlli interni. Sebbene tale competenza si possa desumere da alcuni passaggi del Documento di consultazione, non appare però evidente, *prima facie*, con puro riferimento al *wording*, una chiara attribuzione della responsabilità finale della valutazione della tenuta del sistema dei controlli interni all'organo con funzione di supervisione strategica, come avviene per esempio nel Codice di Autodisciplina.

Per quanto riguarda la nomina dei responsabili delle funzioni di controllo, si rileva (Sez. III, par. 1, lett. b) terzo alinea) che – diversamente da quanto prescritto dalle "*Disposizioni di vigilanza in materia di organizzazione e governo societario delle banche*" che si riferiscono alla revisione interna (Internal Audit) e alla conformità (Compliance) - la competenza in merito alla designazione dei responsabili di revisione interna e di conformità non viene attribuita all'organo amministrativo (*rectius* organo con supervisione strategica), bensì all'organo con funzione di gestione (sia pure d'accordo l'organo con funzione di supervisione strategica e dopo aver sentito l'organo con funzione di controllo).

Come peraltro meglio specificato nella Sezione III, la competenza attribuita all'organo con funzione di supervisione strategica circa la nomina e revoca del responsabile della funzione di revisione interna (Internal Audit) è prevista sia dagli standard professionali dell'Internal Audit che dal Codice di Autodisciplina delle società quotate.

Con riferimento poi al punto "*Nel caso di banche che adottano sistemi interni di misurazione dei rischi per la determinazione dei requisiti patrimoniali, l'organo con funzione di supervisione strategica svolge anche i seguenti compiti:*

- *[…]*
- *con cadenza almeno annuale, esamina i riferimenti forniti dalla funzione di convalida e assume, col parere dell'organo con funzione di controllo, formale delibera con la quale attesta il rispetto dei requisiti previsti per l'utilizzo dei sistemi"*

si fa presente come nella formulazione proposta – che andrà ad abrogare quanto attualmente previsto al Titolo I – Capitolo I – Parte IV pag. 25" della Circ. 263/2006, non sia più presente l'esplicito riferimento alla relazione annuale predisposta dalla revisione interna.

Inoltre considerato quanto sul punto espressamente richiesto al Titolo II (requisiti patrimoniali) – parte II (metodologia basata sui rating interni IRB) della Circ. 263/2006 che – salvo errore resterà vigente – si chiede di confermare se:

- la consueta relazione annuale predisposta dalla funzione di revisione interna sarà da intendersi ancora obbligatoriamente prevista;
- in caso affermativo da indirizzarsi a quali organi aziendali.

Al fine di evitare qualsiasi dubbio interpretativo e/o disallineamento rispetto alla normativa applicabile in materia di continuità operativa, si suggerisce di prevedere un espresso richiamo alle competenze che le disposizioni emanate da codesta Autorità nel luglio 2004 hanno attribuito all'organo con funzione di supervisione strategica introducendo una previsione del seguente tenore: "*L'organo con funzione di supervisione strategica stabilisce gli obiettivi e le strategie di continuità del servizio; assicura risorse umane, tecnologiche e finanziarie adeguate per il conseguimento degli obiettivi fissati, garantendo che il tema della continuità operativa sia adeguatamente considerato a tutti i livelli di responsabilità; approva il piano; viene informato, con frequenza almeno annuale, sulla adeguatezza dello stesso.*"

Più in generale, non è posto chiaramente in evidenza quale differente ruolo dovrebbe essere svolto dall'organo con funzione di supervisione strategica rispetto a quello con funzione di gestione per quanto riguarda la definizione dei compiti e delle responsabilità delle funzioni coinvolte nel processo di gestione dei rischi, anche ai fini della definizione dei flussi informativi interni. Infatti, da un lato, si propone di attribuire all'organo con funzione di supervisione strategica l'approvazione delle funzioni aziendali e societarie di controllo, nonché i relativi compiti e responsabilità mentre, dall'altro, viene attribuito all'organo con funzione di gestione il compito di stabilire le responsabilità delle strutture e delle funzioni aziendali coinvolte nel processo di gestione dei rischi (cfr. par. 3 - pag. 11 alinea c).

Analogamente è attribuita all'organo con funzione di supervisione strategica l'approvazione dei flussi informativi tra le funzioni di controllo e tra queste e gli organi aziendali, mentre l'organo con funzione di gestione definisce "*i flussi informativi interni volti ad assicurare agli organi aziendali e alle funzioni aziendali di controllo la piena conoscenza e governabilità dei fattori di rischio*"(par. 3 - pag. 11 alinea e)). Al fine di evitare dubbi interpretativi, nonché eventuali sovrapposizioni, si suggerisce di rendere maggiormente esplicito il diverso ambito di competenza dei due organi.

1.3 Organo con funzione di gestione

Con riferimento alla seguente previsione:
"*…assicura:*

a) *……..*

b) *l'adeguatezza delle funzioni aziendali di controllo…"*

non è chiaro se trattasi di responsabilità anche di valutazione sull'adeguatezza delle funzioni di controllo. Al fine di evitare dubbi, si suggerisce di precisare che la competenza della valutazione resta in capo all'organo con funzione di supervisione strategica.

Per le medesime ragioni espresse riguardo all'implementazione delle competenze dell'organo di con funzione di supervisione strategica in materia di continuità operativa, si ritiene opportuno esplicitare anche le competenze dell'organo con funzione di gestione in materia di continuità operativa: "*L'organo con funzione di gestione nomina il responsabile del piano di emergenza; promuove il controllo periodico del piano e l'aggiornamento dello stesso a fronte di rilevante 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*".

Non è chiaramente detto, come potrebbe invece desumersi da quanto previsto nella Sez. III, par. 2, primo alinea, se l'organo con funzione di gestione sia il destinatario dei programmi di attività menzionati, insieme agli altri organi aziendali.

1.4 Organo con funzione di controllo

Rispetto alla formulazione in merito alla proposta di attribuire le funzioni dell'organismo di vigilanza previsto ai sensi della D. Lgs. 231/2001 in capo all'organo con funzione di controllo "ove vi siano particolari e motivate esigenze", si chiede di chiarire la natura delle "*particolari e motivate esigenze*" per poter affidare tali funzioni a un organismo appositamente istituito.

Sembra infine rilevante integrare le previsioni in tema di "*organo con funzione di controllo*", con la precisazione che l'organo in esame svolge altresì le funzioni demandate al Comitato per il controllo interno e la revisione contabile di cui all'art.19 del D. Lgs. 39/2010, in quanto le "*banche*" sono, ai fini del predetto Decreto (cfr. art. 16), esplicitamente qualificate come "*enti di interesse pubblico*".

1.5 Il coordinamento delle funzioni di controllo (interne e societarie)

Con specifico riguardo al "*comitato controllo e rischi*", si ritiene necessario eliminare la precisazione in merito alla sua composizione ("*composto da amministratori non esecutivi, in maggioranza indipendenti*"), in quanto solo parzialmente allineata con le previsioni del citato

Codice di Autodisciplina (cfr. Principio 7.P.4). A livello più generale, si ritiene opportuno che il Documento di consultazione in esame faccia esplicito riferimento al ruolo del comitato controllo e rischi quale organo a supporto delle decisioni dell'organo con funzione di supervisione strategica relative al sistema di controllo interno e di gestione di rischi.

Si chiede inoltre di esplicitare il ruolo delle funzioni societarie di controllo (che riportano alle strutture di vertice dell'azienda – ad esempio Dirigente Preposto, Responsabile della Sicurezza sul Lavoro e quello della continuità operativa) con particolare riferimento alla possibile attribuzione di responsabilità analoghe a quelle delle funzioni aziendali di controllo, per specifiche aree alle stesse attribuite dalla legislazione vigente (vds anche nota 11 Provv. Banca d'Italia del 30 marzo 2011 "*Disposizioni in materia di politiche e prassi di remunerazione e incentivazione nelle banche e nei gruppi bancari*").

Con riguardo al "*documento nel quale sono definiti i compiti e le responsabilità di vari organi e funzioni (aziendali e societarie) di controllo (omissis)*", sarebbe opportuno rivedere il processo di approvazione proposto (che richiederebbe l'intervento dell'organo con funzione di supervisione strategica) che in alcuni casi dovrebbe approvare due volte gli stessi contenuti. Infatti, se una delle finalità è quella di un'analisi sull'andamento dei flussi e sulle aree di sovrapposizione e sinergia, questa – attenendo ad un profilo operativo piuttosto astratto – potrebbe essere svolta dalle strutture interessate con il coinvolgimento dell'organo con funzione di gestione, ferma la reportistica all'organo con funzione di supervisione strategica.

Relativamente alla nota 13, si segnala la presenza di un refuso. Si ritiene, infatti, che laddove si rimanda per la descrizione dettagliata ai compiti e poteri dell'organo con funzioni di controllo, debba intendersi "*dei comitati costituiti all'interno dell'organo con funzione di supervisione strategica*".

SEZIONE III - FUNZIONI AZIENDALI DI CONTROLLO

1.1 Istituzione delle funzioni aziendali di controllo

Con riferimento alla Sez. III art. 1 lettera b) "*i responsabili di tali funzioni non devono avere responsabilità diretta di aree operative né devono essere gerarchicamente subordinati ai responsabili di tali aree",* si chiede un chiarimento circa la definizione di "*aree operative*", specificando se tra le aree operative si intenda anche l'attività di erogazione creditizia.

Con riferimento invece alla nomina dei responsabili delle funzioni di controllo si ritiene che l'attribuzione all'organo con funzione di gestione ne limiterebbe l'indipendenza. A supporto di questa interpretazione si riportano:

- le "*Disposizioni di Vigilanza in Materia di Organizzazione e Governo Societario delle Banche*" 4 marzo 2008 che prevedono che "*Oltre alle attribuzioni non delegabili per legge, non possono formare oggetto di delega: le decisioni concernenti le linee e le operazioni strategiche e i piani industriali e finanziari, la nomina del direttore generale, l'assunzione e la cessione di partecipazioni di rilievo, l'approvazione e la modifica dei principali regolamenti interni, l'eventuale costituzione di comitati interni agli organi aziendali, la nomina del responsabile delle funzioni di revisione interna e di conformità. Nell'ambito delle società capogruppo potranno essere delegate le operazioni comportanti variazioni non significative del perimetro del gruppo*",
- gli Standard Internazionali per la Pratica Professionale dell'Internal Auditing nella Guida Interpretativa 1110-1 Indipendenza Organizzativa, prevedono che: "*Si realizza un'indipendenza organizzativa efficace quando il responsabile internal auditing riferisce funzionalmente al board. Esempi di riporto funzionale al board comportano che il board: approvi le decisioni relative alla nomina e all'esonero del responsabile internal auditing*".

Ai riferimenti normativi e agli standard professionali citati a supporto, può, inoltre, aggiungersi il Codice di Autodisciplina delle società quotate, laddove prevede (cfr. Criterio applicativo 7.C.1) che "*Il Consiglio di amministrazione, su proposta dell'amministratore incaricato del sistema di controllo interno e di gestione dei rischi e previo parere favorevole del comitato controllo e rischi, nonché sentito il collegio sindacale, nomina e revoca il responsabile della funzione di internal audit*".

Per quanto precede, le banche quotate che avessero già adottato il Codice di Autodisciplina introducendo tale raccomandazione si troverebbero poi, in attuazione delle disposizioni in esame, a dover fornire una "*explanation*" di "*non compliance*" al Codice stesso.

Si propone dunque che la nomina e revoca siano deliberate dall'organo con funzione di supervisione strategica, su proposta dell'organo con funzione di gestione e sentito l'organo con funzione di Controllo.

Nel caso di affidamento in service delle funzioni di controllo alla capogruppo, la previsione della necessità di un referente "*incaricato della complessiva supervisione della specifica attività di controllo internalizzata*" appare eccessiva e fuorviante nei meccanismi di relazione con la capogruppo. In tale ipotesi, il referente dovrebbe svolgere una funzione di supporto all'outsourcer piuttosto che un compito di controllo del rispetto dei livelli di servizio da parte del medesimo. Si propone dunque una riformulazione delle previsioni regolamentari in tal senso.

1.2 Programmazione e rendicontazione dell'attività di controllo

Non appare chiarissimo il riferimento al "*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*", per quanto concerne la funzione di controllo dei rischi (*risk management*). Sarebbe auspicabile chiarire se si faccia riferimento ai piani di risoluzione delle eventuali carenze riscontrate nell'ambito della attività di verifica della conformità alle norme e di controllo dei rischi e ai piani relativi ai progetti attivati dalla banca per migliorare e rafforzare il sistema dei controlli oppure se si faccia riferimento al "*piano delle attività di verifica e di controllo*". In quest'ultimo caso, occorrerebbe sottolineare che alcune attività di controllo e di verifica hanno natura continuativa e altre sono attivate da richieste o eventi specifici. Si fa presente che la pianificazione di queste attività è di difficile attuazione.

In merito al piano di audit, si chiede di precisare il contenuto minimo della specifica sezione relativa all'attività di revisione interna del sistema informativo (*ICT auditing*) in quanto da una mera elencazione nel piano operativo degli interventi di audit pianificati, potrebbe risultare una forma di rappresentazione non sufficientemente *compliant* con quanto espressamente richiesto dall'Autorità di Vigilanza.

Relativamente ai flussi informativi richiesti a ciascuna funzione aziendale di controllo, suggeriamo – per maggiore chiarezza – di specificare che il programma di attività, la relazione dell'attività svolta e la situazione dei controlli interni, possano essere contenuti anche in un singolo documento (ad esempio, come avviene già con il Documento interno annuale della funzione di compliance).

Da ultimo, laddove si prevede che le funzioni di controllo "*riferiscono, ciascuna per gli aspetti di rispettiva competenza, in ordine alla completezza, adeguatezza ed affidabilità del sistema dei controlli interni*", non è chiaro se il termine "*affidabilità*" sia da intendersi quale sinonimo di "*funzionalità*", termine impiegato in altri casi, o in generale di "*efficacia*".

1.3 Requisiti specifici delle funzioni aziendali di controllo

1.3.1 Premessa

Nessuna osservazione

1.3.2 Funzione di conformità alle norme (compliance)

In relazione alla previsione che la funzione di compliance "*presiede alla gestione del rischio di non conformità alle norme con riguardo a tutta l'attività aziendale*", riteniamo opportuno sia specificato in dettaglio a quali attività si intenda fare riferimento. Se essa dovesse implicare l'estensione dell'attività della funzione a tutte le normative che riguardano l'attività della banca, non si ritiene di

concordare con tale previsione, che di fatto porta a riconoscere alla funzione un perimetro non più definito. A nostro avviso infatti, l'approccio prevalente, sia a livello nazionale sia all'estero, vede la focalizzazione della funzione di compliance su un perimetro definito, prevedendo al contempo il presidio del rischio di non conformità anche da parte di altre funzioni aziendali per aree a contenuto specialistico, ovvero per le quali la stessa normativa primaria identifica specifiche responsabilità (ad esempio Dirigente Preposto, Responsabile della Sicurezza sul Lavoro). La mancata definizione di un perimetro definito comporterebbe inoltre, significativi impatti in termini di incremento di risorse e di nuove competenze, peraltro spesso di difficile reperimento e con il rischio di creare duplicazione di attività. Pertanto, si suggerisce che sia comunque riconosciuta agli intermediari la facoltà di attribuire, per alcune aree specialistiche, la responsabilità sulla gestione del rischio di non conformità anche ad altre funzioni aziendali, al caso prevedendo l'istituzione al loro interno di una struttura dedicata al presidio del rischio di non conformità, indipendente dalle strutture operative delle funzioni medesime e con riporti diretto al responsabile delle stesse.

Si ritiene non praticabile, inoltre, in un gruppo della nostra dimensione e articolazione, il ricorso a meccanismi di presidio "indiretto" da parte della compliance sulle menzionate aree non coperte, in quanto, in assenza di adeguate strutture interne (in termini di risorse e professionalità), il presidio di compliance risulterebbe esclusivamente di carattere formale.

Le considerazioni di cui sopra sono, a nostro avviso, ancor più appropriate se riferite alla normativa fiscale, dato il carattere altamente specialistico della stessa. Al riguardo, inoltre si segnala come sia all'esame del Parlamento il disegno di legge delega – atto C. 5291 - in corso di approvazione e recante "*Disposizioni per un sistema fiscale più equo, trasparente e orientato alla crescita*", che riguarda anche l'attribuzione di responsabilità in merito, nel quadro del complessivo sistema dei controlli interni.

Si suggerisce, pertanto, di rinviare la definizione del suddetto punto in discussione fino a quando il Legislatore non si sarà espresso sull'argomento, evitando così il rischio che gli intermediari finanziari si trovino di fronte a disposizioni di vigilanza non coerenti, in tutto o in parte, con la predetta emananda legge delega.

Si chiedono chiarimenti relativamente alla previsione contenuta nella nota 20, tenuto conto che alla banca non possono essere attribuiti poteri di controllo tributario e relative responsabilità nei confronti della clientela.

Relativamente ad alcune previsioni contenute nel paragrafo in commento si segnala in particolare che:

- non ci risulta di immediata comprensione cosa si intenda per "*ausilio alle strutture aziendali per la definizione delle metodologie di valutazione dei rischi di non conformità alle norme*". Infatti, a nostro parere, alla funzione di compliance dovrebbe essere attribuito il ruolo di definire le metodologie di valutazione dei rischi di non conformità, piuttosto che quello di supportare altre strutture aziendali in tale attività;
- ci sembra che, tra gli adempimenti citati, non vi siano sostanziali differenze tra "*l'individuazione di idonee procedure per la prevenzione del rischio rilevato con possibilità di richiederne l'adozione*" e "*la proposta di modifiche organizzative e procedurali finalizzate ad assicurare un adeguato presidio dei rischi di non conformità identificati*".

Si segnala altresì che l'elenco degli adempimenti di cui al paragrafo in commento non contempla l'attività di controllo ex post nel continuo, oramai entrata nella prassi operativa della funzione, peraltro già attribuita formalmente da alcune normative di Vigilanza (quali ad esempio, la Trasparenza, l'Antiriciclaggio e la MiFID).

1.3.3 Funzione di controllo dei rischi (risk management function)

Non si condivide appieno la previsione secondo la quale il responsabile della funzione di controllo dei rischi possa essere collocato alle "dirette dipendenze" del Comitato Controlli Interni & Rischi (IC&RC): ciò in quanto, in UniCredit, i comitati consiliari sono organi consultivi o propositivi rispetto

alle decisioni che rimangono in capo al consiglio. Inoltre, l'eventuale "dipendenza" diretta (sotto che profilo, gerarchico? funzionale? di mero indirizzo?) del *Chief Risk Officer* solo nei confronti di un gruppo ristretto di amministratori non appare coerente con il maggior coinvolgimento nelle tematiche di *risk management* attribuite al consiglio. A maggior ragione non si condivide la previsione di collocazione obbligatoria dell'intera funzione alle dirette dipendenze dei citati organi, in caso di banche classificate ai fini SREP 1 e 2. Infine non si comprende il razionale per il quale il riporto al consiglio o al comitato controlli interno e rischi sia previsto per le funzioni di *risk management* e revisione interna e non per la funzione di conformità.

UniCredit condivide la finalità di rafforzare la funzione di controllo dei rischi come chiaramente emerge dal Documento di consultazione, peraltro in linea con il "pacchetto" CRD IV (Regolamento e Direttiva) tuttora all'esame delle istituzioni. In tale ambito è esplicitato il principio di "accesso diretto" del responsabile della funzione di controllo (art. 75, 5: "*the head of the risk management function (…) shall be able to have direct access to the management body in its supervisory function when necessary*"). UniCredit è concorde nell'esplicitare tale principio.

Inoltre ci sembra che l'attuale impostazione della normativa includa la valutazione e il monitoraggio del "rischio modello" nell'ambito della disciplina sul trattamento dei singoli profili di rischio di primo pilastro. La valutazione complessiva del rischio è funzionale alla determinazione del *capital cushion* nell'ambito della disciplina sul processo di controllo prudenziale. Posto che la nuova normativa oggetto di consultazione non intende intervenire sulla disciplina dei requisiti patrimoniali di primo pilastro né su quella del processo di controllo prudenziale (secondo pilastro), non appare chiaro se la nuova normativa sul sistema dei controlli intenda suggerire soluzioni organizzative specifiche rispetto alla misurazione e al monitoraggio del rischio di modello.

In merito ai pareri preventivi sulla coerenza con la politica di governo dei rischi delle operazioni di maggiore rilievo, si ritiene necessario una volta esplicitato con maggiore definizione il concetto delle operazioni di maggior rilievo, indicare gli ambiti rilevanti ai fini del parere preventivo.

1.3.4 Funzione di revisione interna (internal audit)

Nell'ambito delle attività attribuite alla funzione di revisione interna viene richiesto – tra l'altro –di portare all'attenzione degli organi aziendali i possibili miglioramenti, con particolare riferimento alle politiche di governo dei rischi, al processo di gestione dei rischi, nonché agli strumenti di misurazione e controllo degli stessi. E' stato, quindi, introdotto il concetto di "*politiche di governo dei rischi*" in sostituzione al concetto di "*politiche di gestione dei rischi*". Si ritiene opportuno chiedere precisazioni in merito.

Il Documento di consultazione demanda alla funzione di compliance il compito di verificare che le procedure interne siano coerenti con l'obiettivo di prevenire la violazione di norme esterne (leggi e regolamenti) o di autoregolamentazione, applicabili alle banche. Da tale previsione potrebbe emergere una possibile area di sovrapposizione con la funzione di compliance. Si richiede, pertanto, di meglio precisare il perimetro di attribuzione dei controlli ex post sulle norme per le funzioni di compliance e di internal audit.

Inoltre, per enfatizzare l'importanza che la pianificazione dell'attività debba essere strettamente correlata ai rischi, si suggerisce di integrare la parte finale del bullet a) come segue: "*La frequenza delle ispezioni deve essere coerente con l'attività svolta e il relativo livello di rischi*"'. Poiché la funzione di revisione interna, per poter adempiere in modo efficiente ed efficace al proprio ruolo, deve poter avviare gli accertamenti in autonomia e non solo se c'è una espressa richiesta degli organi aziendali, si propone di modificare il testo come segue: "*espleta inoltre compiti d'accertamento con riguardo a specifiche irregolarità anche ove richiesto dagli organi aziendali*".

Si condivide la collocazione organizzativa del responsabile della funzione di revisione interna a riporto dell'organo con funzione di supervisione strategica. Riteniamo, invece, che attribuire all'organo con funzione di gestione le prerogative "*di concorrere all'indirizzo dell'attività di revisione interna*" possa rappresentare una limitazione all'indipendenza della funzione medesima. Al

riguardo, si ritiene opportuno formulare una proposta di modifica al testo eliminando "*al fine di concorrere all'indirizzo dell'attività di revisione interna*".

Sul punto relativo agli esiti degli accertamenti, il Documento di consultazione cita genericamente gli organi aziendali, il che – a rigore – vorrebbe dire che gli esiti degli accertamenti conclusisi con giudizi negativi o che evidenzino carenze di rilievo dovranno essere trasmessi integralmente, tempestivamente e direttamente a tutti gli organi aziendali (con funzione di supervisione strategica, di gestione e controllo). Premesso che si ravvisa l'opportunità di specificare "*nel caso di rischi rilevanti*", sarebbe altresì opportuno sul punto, chiarire se per organi aziendali ci si vuole effettivamente riferire indistintamente a tutti i citati organi e se la trasmissione degli accertamenti conclusisi con giudizi negativi - o che evidenzino carenze di rilievo - dovrà indiscriminatamente avvenire per tutti i citati organi integralmente, tempestivamente e direttamente. Detti requisiti appaiono troppo stringenti in generale e, per gruppi di grandi dimensioni o presenti su diversi Paesi, rappresenterebbero prescrizioni eccessivamente onerose in termini di impatto operativo/ gestionale. Si propone pertanto di:

- implementare il testo specificando "*nel caso di rischi rilevanti*";
- eliminare "*integralmente, tempestivamente e direttamente*" o prevedere almeno un riferimento generico: i) alla sintesi degli accertamenti conclusi, e ii) al principio di proporzionalità in relazione alla dimensione aziendale e alla conseguente numerosità dei flussi di reporting prodotti;
- chiarire a quali organi ci si vuole riferire;
- chiarire se il riferimento si estende anche agli accertamenti conclusi nelle società del gruppo dalle funzioni locali di audit.

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

Si raccomanda al punto "*Fermo restando la reciproca indipendenza e rispettivi ruoli aziendali, le funzioni aziendali di controllo collaborano tra loro e con le altre funzioni (es. funzione legale, organizzazione, sicurezza informatica) allo scopo di sviluppare le proprie metodologie di controllo..*" di non far riferimento esclusivamente alla sicurezza informatica, bensì alla sicurezza in generale, eliminando dalla frase il termine "*informatica*".

SEZIONE IV - ESTERNALIZZAZIONI DI FUNZIONI AZIENDALI (OUTSOURCING)

1.1 Principi generali e requisiti particolari

Pur condividendo il principio che la banca che ricorre all'esternalizzazione debba mantenere la capacità di controllo e la responsabilità sulle attività esternalizzate, si ritiene opportuno modulare l'intera normativa sull'outsourcing in due livelli separati, con un maggiore livello di interferenza/controllo se l'outsourcing è verso società non appartenenti al Gruppo Bancario e un livello meno articolato nel caso di outsourcing con società appartenenti al Gruppo.

Non pare a nostro avviso del tutto sostenibile la previsione della "*necessità di mantenere nella banca le competenze tecniche e gestionali essenziali per re-internalizzare, in caso di necessità, il loro svolgimento*": si ritiene opportuno precisare che cosa si intenda per "*competenze tecniche e gestionali essenziali*". Il mantenimento di competenze tecniche / gestionali per attuare una eventuale re-internalizzazione, "*in caso di necessità*" e potenzialmente dal "giorno zero", avrebbe un costo significativo non coerente con la scelta strategica effettuata.

Si ritiene comunque che la politica aziendale delineata in materia di esternalizzazione sia troppo onerosa per una funzione aziendale non importante. Si propone quindi di precisare che le regole della Sezione in discorso non si applicano all'esternalizzazione di funzioni non importanti, atteso

che CEBS 2006 (Guideline 5) raccomanda che "*There should be no restrictions on the outsourcing of non-material activities of an outsourcing institution*".

In tema di re-internalizzazione delle attività esternalizzate, si chiede di precisarne modalità e termini della stessa, atteso che (i) CEBS 2006 (Guideline 8, paragrafo 2, lett. d) richiede soltanto che "*[…] the contract should include a termination and exit management clause, where proportionate and if deemed necessary, which allows the activities being provided by the outsourcing service provider to be transferred to another outsourcing service provider or to be reincorporated into the outsourcing institution*" e (ii) the Joint Forum of Basel Committee on Banking Supervision, IOSCO and International Association of Insurance Supervisors, Outsourcing in Financial Services, pag. 15, prevede che "*Contingency plans, in the event of deteriorating performance, must account for the costs of alternative options. In the face of unsatisfactory responsiveness from the service provider, a regulated entity's options include changing service providers, moving the activity internally to the institution, or sometimes even exiting the business*[1]."

Si chiede inoltre di precisare se, tra gli eventi che potrebbero compromettere la capacità del fornitore di garantire il servizio – da prevedere tra le clausole obbligatorie del contratto – debbano essere in ogni caso compresi:

- le performance finanziarie;
- i mutamenti importanti nella struttura organizzativa e proprietaria del fornitore,

atteso che CEBS 2006 (Guideline 6, paragrafo 4) richiede, al riguardo, che tali eventi siano "*appropriately monitored and assessed by the outsourcing institution's management so that any necessary corrective measures can be taken promptly*". La previsione delle predette clausole nel contenuto minimo obbligatorio del contratto di esternalizzazione potrebbe determinare, da un lato, il vantaggio di (i) esentare la banca da responsabilità per non aver adeguatamente gestito il rischio di controparte e di (ii) consentire l'immediata risoluzione del contratto al verificarsi dei suddetti eventi; dall'altro, il costo connesso con il monitoraggio del fornitore attraverso l'esame della situazione finanziaria (bilanci) e proprietaria (visure).

In merito all'obbligo di comunicazione da parte del fornitore al verificarsi di incidenti, UniCredit ritiene che l'obbligo, previsto da tale norma, debba essere esteso a tutti gli incidenti e non solo a quelli di sicurezza.

La disciplina inoltre prevede che "*la banca 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 interessi 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")*". Al riguardo:

- si chiede di precisare che eventuali conflitti di interesse con l'outsourcer debbano essere individuati e gestiti (attraverso apposite procedure interne), pur non essendo vietati (sul punto, cfr. pure Regolamento Congiunto, art. 23),
- si suggerisce, pur condividendo tale previsione (peraltro già utilizzata per alcune esternalizzazioni) di prevedere la possibilità – nelle realtà più complesse - che vengano istituiti più referenti (e non "un responsabile del controllo delle singole funzioni esternalizzate") in funzione della tipologia delle attività esternalizzate.

Si propongono pertanto le seguenti modifiche al bullet "*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 interessi dell'outsourcer; in tale ambito, individua, all'interno della propria organizzazione, i responsabili del controllo delle singole funzioni esternalizzate dotati di adeguati requisiti di professionalità ("referenti per le attività esternalizzate")*".

In merito al fatto che "*Le banche che intendono esternalizzare, in tutto o in parte, lo svolgimento di funzioni operative importanti o di controllo sono tenute a informare preventivamente la Banca d'Italia….*" si ritiene utile, anche tenuto conto di quanto previsto dalle linee guida CEBS 2006[2], di limitare l'obbligo di informativa preventiva alle sole esternalizzazioni presso soggetti aventi sede nei paesi extra UE.

Si suggerisce infine di integrare la disposizione normativa, prevedendo anche la possibilità che la relazione da trasmettere alla Banca d'Italia entro il 30 aprile di ogni anno possa essere redatta dall'outsourcer in coordinamento con il referente aziendale, in analogia, ad esempio, al modello di outsourcing delle attività di Compliance per le entità italiane attualmente in vigore nel Gruppo.

Da ultimo si ritiene che la predisposizione della Relazione da parte della funzione di revisione interna da trasmettere alla Banca d'Italia entro il 30 aprile di ogni anno debba essere, *in primis*, in carico al responsabile del controllo delle singole funzioni esternalizzate (i.e. referente aziendale per le attività esternalizzate), eventualmente corredata dalle considerazioni della funzione di revisione interna. In ogni caso, le considerazioni dell'Internal Audit saranno comunque limitate ai risultati emersi dalle attività previste nel piano annuale di audit. Si propone una formulazione in tal senso.

1.2 Esternalizzazione del trattamento del contante

Nessuna osservazione

SEZIONE V - IL SISTEMA DEI CONTROLLI INTERNI NEI GRUPPI BANCARI

1.1 Ruolo della Capogruppo

Nessuna osservazione

1.2 Controlli interni di Gruppo

La disciplina prevede che la Capogruppo convalidi i processi di gestione dei rischi all'interno del gruppo; si chiede di precisare il significato del termine "*convalida*".

Inoltre, dalla esperienza maturata dal Gruppo UniCredit, le attività relative alla "*fissazione dei criteri di valutazione delle posizioni e la creazione di una base informativa comune che consenta a tutte le società appartenenti al gruppo di conoscere l'esposizione dei clienti nei confronti del gruppo nonché le valutazioni inerenti alle posizioni dei soggetti affidati*" potrebbero risultare limitate dalla presenza di vincoli restrittivi sulla distribuzione delle informazioni imposti dalle normative nazionali dei paesi in cui operano le società del Gruppo.

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

- *[…]*
- *le decisioni strategiche in merito all'utilizzo di strutture accentrate sono riservate all'organo con funzione di supervisione strategica con il parere dell'organo con funzione di controllo della capogruppo",*
- *[…]*

2 CEBS 2006 (Guideline 4, paragrafo 4) prevede che *"Subject to the principles that apply to crossborder outsourcing expressed under Guideline 4.1(i), no special rules are needed in relation to the geographical location of an outsourcing service provider. However, due to possible data protection risks and risks to effective supervision by the supervisory authority, institutions should take special care when entering into and managing outsourcing agreements that are undertaken outside the EEA".*

Con riferimento alle "*decisioni strategiche in merito all'utilizzo…*" si auspica che si intenda la definizione del modello di presidio a livello di gruppo e non invece la decisione di accentramento di una funzione (ad es. Compliance) riferita a ogni società del Gruppo (nella quale viene implementato in concreto un modello precedentemente approvato), che invece parrebbe soluzione onerosa e non efficiente.

Con riferimento al passaggio "*riportano funzionalmente e gerarchicamente a quest'ultima*", sarebbe opportuno precisare l'ammissibilità anche di un modello alternativo rispetto a quello prospettato che prevede il riporto gerarchico del referente alla società esternalizzante ed un riporto manageriale / funzionale verso la struttura della società che svolge il servizio in outsourcing come ad esempio avviene per la funzione di Compliance in UniCredit nei confronti delle altre Entità italiane del Gruppo. Inoltre per la fattispecie prevista dal testo in consultazione andrebbe precisato che la società esternalizzante deve mantenere un presidio di monitoraggio delle prestazioni della funzione di controllo esternalizzata in quanto responsabile primario del presidio dei propri rischi.

In generale si ritiene necessario poter individuare un referente per ciascuna funzione di controllo, non limitandosi esclusivamente a un unico referente.

Inoltre, le disposizioni prevedono che in capogruppo ci sia separazione tra le unità e le risorse che erogano attività di audit in service (base individuale) e quelle responsabili dei controlli su base consolidata che devono verificare la funzionalità complessiva del sistema dei controlli interni. Occorrerebbe chiarire in modo esplicito le modalità e i meccanismi di funzionamento e di governo che l'audit "*su base consolidata*" deve adottare. Tale impostazione appare di significativo pregiudizio per l'efficienza e l'efficacia delle attività di revisione interna per i gruppi a maggior articolazione organizzativa, laddove la decisione dell'insourcing intenda perseguire anche obiettivi di economicità e di efficienza.

In ultima istanza ravviseremmo l'applicabilità di quanto proposto nel Documento di consultazione esclusivamente nel perimetro delle società bancarie del Gruppo e non anche in quello delle società strumentali o di servizi.

Riepilogando, per quanto riguarda l'Internal Audit si propone di:

- chiarire le modalità e i meccanismi di funzionamento e di governo dell'audit "*su base consolidata*";
- modificare nella salvaguardia della responsabilità nell'esecuzione delle attività di audit esternalizzate, il testo proposto prevedendo l'identificazione di un referente interno alla capogruppo limitatamente alle attività svolte per conto di banche/finanziarie;
- eliminare la separazione tra le unità e le risorse deputate a svolgere l'internal audit su base individuale e consolidata.

Infine, assumendo che la prescrizione si riferisca alle sole componenti italiane del Gruppo, come sembrerebbe emergere dai capitoli successivi, riteniamo che non sia necessaria l'informativa preventiva a Banca d'Italia quando l'esternalizzazione avvenga all'interno del Gruppo.

SEZIONE VI - IMPRESE DI RIFERIMENTO

1.1 Imprese di riferimento

Nessuna osservazione

SEZIONE VII - PROCEDURA DI ALLERTA INTERNA

Si condivide il principio alla base della presente procedura, ma si richiede di specificare se con il riferimento a "*eventuali disfunzioni dell'assetto organizzativo o del sistema dei controlli interni* " si

intenda prevedere che, oltre alla segnalazione di comportamenti illeciti/non conformi, possano essere segnalate anche le "*eventuali*" inefficienze organizzative, a prescindere quindi da requisiti di illiceità, di violazione di norme o di non conformità.

Laddove l'interpretazione fosse quella più estensiva si ritiene di segnalare che tale approccio sarebbe a nostro avviso troppo oneroso e - in assenza di una chiara definizione dei livelli di importanza/gravità - anche inefficace, in quanto potrebbe ridurre la capacità della procedura stessa di fare emergere gli aspetti veramente significativi in termini di violazione delle norme. Si suggerisce pertanto, in linea con la prassi a livello internazionale in tema di Whistleblowing, di privilegiare l'approccio più restrittivo, lasciando le segnalazioni relative a disfunzioni organizzative o del sistema dei controlli interni alle procedure ordinarie degli intermediari.

SEZIONE VIII - SUCCURSALI DI BANCHE COMUNITARIE E DI BANCHE EXTRA COMUNITARIE AVENTI SEDE NEI PAESI DEL GRUPPO DEI DIECI O IN QUELLI INCLUSI IN UN ELENCO PUBBLICATODALLA BANCA D'ITALIA

Partendo dal presupposto che la sezione si riferisce a succursali di banche estere operanti in Italia, si chiede di chiarire se il "*legale rappresentante*" sia quello della succursale o il legale rappresentante della banca.

Sarebbe poi opportuno dettagliare i criteri in base ai quali condurre la verifica di conformità, anche al fine di calibrare l'attività richiesta in base all'effettiva operatività delle succursali estere.

SEZIONE IX - INFORMATIVA ALLA BANCA D'ITALIA

Con riguardo ai rapporti tra la funzione di revisione interna e l'Autorità di Vigilanza, si suggerisce in linea con quanto formulato nel Documento BCBS "*The internal audit function on banks*" di prevedere nel presente paragrafo uno specifico riferimento ai canali di comunicazione di Internal Audit con il *Supervisor*. In particolare, si riterrebbe opportuna un'informativa, quando necessaria, dall'Autorità di Vigilanza alla funzione di revisione interna relativamente a eventuali aree di rischio meritevoli di attenzione.

Si suggerisce di integrare la disposizione normativa, prevedendo anche la possibilità che la relazione possa essere redatta dall'outsourcer in coordinamento con il referente aziendale, in analogia al modello di outsourcing delle attività di Compliance per le entità italiane attualmente in vigore nel Gruppo.

Dalla lettura del Documento in consultazione si evince che i documenti citati nella presente Sezione e da trasmettere, debbano essere quelli relativi a tutte le banche del gruppo, italiane ed estere. Questo comporterebbe una serie di problematiche attinenti alla lingua, alla tempistica per il recupero dei documenti, alla numerosità e corposità del materiale da trasmettere, ecc.

A questo proposito si suggerisce di prevedere che la relazione predisposta dalla capogruppo rappresenti anche una sintesi dei principali aspetti inerenti alle entità del gruppo senza l'obbligo di trasmissione di tutti i documenti, in conformità a quanto previsto nell'ultimo capoverso di pagina 33. In alternativa si suggerisce di prevedere una relazione *ad hoc* che sintetizzi i principali aspetti rilevati nei documenti delle entità o di limitare l'obbligo di trasmissione alle sole entità del gruppo aventi sede in Italia.

UniCredit ad esempio provvede già da ora a trasmettere a Banca d'Italia il Documento Interno della funzione di Compliance che illustra gli aspetti principali rilevati per le entità italiane a livello di Gruppo. Non vengono invece inviati i documenti delle singole entità per i quali si rinvia alle considerazioni di cui al precedente punto. Si suggerisce pertanto di prevedere l'obbligo di trasmissione per il solo documento della capogruppo o, sempre in analogia con il precedente punto, estendere l'obbligo di invio alle sole entità del gruppo aventi sede in Italia.

Parimenti, la funzione di Internal Audit di UniCredit trasmette annualmente e periodicamente a Banca d'Italia la relazione annuale che riporta i risultati dell'attività di audit svolta sulla capogruppo e dalle funzioni locali presso le società controllate.

Infine, l'ultimo paragrafo della sezione appare essere una ripetizione rispetto a quanto riportato alla Sezione VIII "*Succursali di banche comunitarie e di banche extracomunitarie aventi sede nei paesi del Gruppo dei Dieci o in quelli inclusi in un elenco pubblicato dalla Banca d'Italia*".

SEZIONE X - DISPOSIZIONI ABROGATE

Nessuna osservazione

ALLEGATO A - DISPOSIZIONI SPECIALI RELATIVE A PARTICOLARI CATEGORIE DI RISCHIO

In merito al rischio di credito e di controparte (paragrafo 2), si chiede un chiarimento circa la funzione aziendale di controllo alla quale è demandato il compito di verifica periodica dell'intero processo di gestione del rischio di credito e di controparte. Dal Documento di consultazione sembrerebbe che la funzione sia quella di Internal Audit.

In tal caso, rispetto al processo di gestione del rischio di credito e controparte sembra riaffermarsi un concetto di periodicità al posto di un approccio *risk based*. Si chiede un chiarimento in tal senso.

ALLEGATO B - CONTROLLI SULLE SUCCURSALI ESTERE

In merito alla disciplina prevista nell'Allegato, si segnala che la conformità alla normativa dei Paesi esteri non può essere compiuta dalla capogruppo in via diretta.

In particolare, le succursali di UniCredit SpA sono assoggettate alle verifiche da parte delle funzioni di controllo locale di secondo livello (Compliance / Risk Management) e di terzo (Internal Audit).

Inoltre, in alcuni casi, UniCredit ha esternalizzato alcuni controlli alle funzioni di controllo di altre società del Gruppo presenti sulle piazze locali. Le Succursali sono assoggettate alle verifiche in loco da parte della funzione di Internal Audit della capogruppo, mirate alla verifica dell'adeguatezza del sistema dei controlli interni della filiale e dell'adeguatezza della stessa funzione di Internal Audit locale.

In merito alla necessità di "*istituire presso le succursali con una operatività significativa un'unità incaricata dei controlli di secondo livello e un'unità avente funzioni di revisione interna. Gli addetti a tali unità, di norma gerarchicamente dipendenti dalle funzione aziendali di controllo centrali, riferiscono, oltre che ai responsabili di tali funzioni, attraverso specifiche relazioni direttamente al dirigente preposto alla succursale capo-area, ove esistente, e all'organo con funzione di gestione*" si suggerisce di non definire in modo rigido la tipologia di riporto tra le funzioni locali di controllo e le funzioni centrali, salvo il principio condivisibile delle doppie linee di riporto (che constano nel riporto verso il dirigente preposto alla succursale e verso le strutture di controllo centrali).

Nel caso di UniCredit SpA, il riporto delle funzioni di controllo delle Succursali è manageriale o funzionale verso le strutture centrali e gerarchico o amministrativo verso il dirigente preposto alla Succursale. Inoltre, nei casi in cui UniCredit ha esternalizzato alcuni controlli alle funzioni di controllo di altre società del Gruppo presenti su piazza, la linea di riporto è tra la funzione incaricata e la rispettiva funzione centrale della casa madre (società del Gruppo).

In merito poi al compito di "*effettuare il controllo documentale su tutti gli aspetti dell'operatività ed estenderlo anche al merito della gestione in modo da condurre ad una valutazione complessiva dell'andamento delle succursali estere, sotto il profilo del reddito prodotto e dei rischi assunti*" si chiede di precisare meglio quale funzione (o è da intendersi che siano le diverse funzioni competenti sulle varie tematiche oggetto di controllo?) sia deputata allo svolgimento delle verifiche descritte e debba riferire sull'esito delle stesse sotto il profilo del reddito e dei rischi all'organo con funzione di supervisione strategica.

Inoltre, dal punto di vista fiscale, la conformità alla normativa fiscale dei Paesi esteri non può essere compiuta dalla capogruppo in via diretta. La stessa deve essere garantita:

- dalla presenza della funzione fiscale nella succursale stessa, nel caso di succursale di più rilevante dimensione;
- dal soggetto esterno al quale sono stati contrattualmente affidati gli adempimenti previsti dalla normativa, nel caso di succursale di minori dimensioni;
- dal controllo di secondo livello, in entrambi i casi sopra citati.

E' inoltre indicato nel Documento di consultazione che la funzione di revisione interna deve verificare *inter alia* l'inserimento sul mercato della succursale estera. Non è chiaro quale rischio si intenda in tal modo presidiare (strategico?).

Si ritiene, peraltro, che non debba essere demandata all'organo con funzione di gestione la fissazione della periodicità delle verifiche che la funzione di revisione interna deve condurre.

Si ritiene quindi opportuno:

- chiedere chiarimenti in ordine alle attività di verifica richieste sull'inserimento sul mercato;
- proporre l'eliminazione dal testo della dicitura "*fissata dall'organo con funzione di gestione*".

TITOLO V – CAPITOLO 8 SISTEMA INFORMATIVO

SEZIONE I - DISPOSIZIONI DI CARATTERE GENERALE

Nessuna osservazione

SEZIONE II - GOVERNO ED ORGANIZZAZIONE DELL'ICT

1.1 Compiti dell'organo con supervisione strategica

Nessuna osservazione

1.2 Compiti dell'organo con funzione di gestione

Il Documento di consultazione prevede tre organi o strutture aziendali distinti per il governo dell'Information & Communication Technology: l'organo con funzione di supervisione strategica, l'organo con funzione di gestione e la funzione ICT. Riconoscendo nelle società a struttura "tradizionale" il consiglio di amministrazione quale organo di supervisione strategica della capogruppo, pare meno evidente, riconoscere l'organo con funzione di gestione che avrebbe la responsabilità, ad esempio, di:

- disegnare e seguire l'implementazione dei processi di gestione dell'ICT;
- approvare gli standard di *data governance*, le procedure di gestione dei cambiamenti (*change management*) e degli incidenti;
- assumere decisioni tempestive in merito a gravi incidenti

oltre a disporre delle competenze tecniche e manageriali coerenti con i compiti assegnati.

Si ritiene che, in realtà dimensionalmente articolate come quella di UniCredit, possa essere prevista la possibilità che i compiti, assegnati nel Documento di consultazione all'organo con funzione di gestione, vengano attribuiti a figure di vertice quali il *Chief Operating Officer* (COO). Ciò anche a garanzia di un forte coordinamento con la funzione di Organizzazione.

1.3 Organizzazione della funzione ICT

Per quanto attiene alla specifica funzione ICT e alla proposta di formalizzazione del ruolo del "*Direttore dei sistemi informativi*", vi e' la previsione che tale funzione abbia una linea di riporto diretto con l'organo con funzione di gestione Il modello organizzativo di UniCredit prevede un'area (Global Banking Services "GBS" - area in responsabilità al *Chief Operating Officer*) per la gestione integrata e sinergica di tutte le componenti della macchina operativa, incluso l'ICT. In tale contesto vale la considerazione sopra esposta che in realtà dimensionalmente articolate come UniCredit, organi e ruoli apicali come il *Chief Operating Officer* di capogruppo dovrebbero poter essere assimilabili a organi con funzione di gestione per le tematiche di competenza (ferma la formalizzazione di opportune deleghe).

Riterremmo inoltre opportuno, relativamente al Capitolo 3 - Organizzazione della funzione ICT ultimo alinea ("*fermo restando quanto previsto nel Capitolo 7, Sezione III […] alle funzioni operative*"), un chiarimento in merito all'attribuzione formale dei compiti di analisi del rischio informatico, in particolare per quanto riguarda il sopraccitato rimando per le funzioni aziendali di controllo. In merito si richiama quanto già evidenziato sulla possibilità di assegnare alle stesse tale responsabilità, anche con riferimento alla necessità di *skills* altamente specialistici.

SEZIONE III - LA GESTIONE DEL RISCHIO INFORMATICO

Pur condividendo il principio sostenuto nel Documento di consultazione, si segnala la difficoltà nell'identificazione dei rischi potenziali e residui connessi al sistema informativo nel suo complesso.

Si ritiene opportuno indicare esplicitamente che la gestione del rischio informatico debba essere integrato nel *framework* della gestione del rischio operativo per evitare *framework* di controllo paralleli e quindi ridondanti.

Si suggerisce di chiarire maggiormente il ruolo che l'utente responsabile deve avere soprattutto in relazione alla funzione di gestione dei rischi.

Non è chiaro infine se la valutazione in capo all'utente responsabile sostituisca quella in capo alla funzione di controllo competente o se invece sia indicata un'unica valutazione aziendale che preveda la responsabilità ultima della valutazione in capo all'utente responsabile.

Inoltre si ritiene che nell'attività di valutazione del rischio potenziale cui sono soggette le risorse informatiche in caso di nuovi sistemi e di rilevanti modifiche ai sistemi esistenti, sia opportuno dare la possibilità all'organo competente (quale misura di appetito al rischio) di definire una soglia per includere nell'analisi solo i sistemi informativi critici per la banca e/o le modifiche da ritenersi significative. Ciò al fine di evitare di avere un eccessivo appesantimento dei processi di cambiamento aziendali, senza veri benefici in termini di controllo e consapevolezza degli aspetti di rischio.

In merito al rischio potenziale, si ritiene eccessivamente dispendioso e di utilità non chiara, doverlo valutare "*prima dell'applicazione degli opportuni presidi di sicurezza*" qualora questo significhi valutare il rischio al lordo di azioni mitiganti già in essere, ovvero valutare una situazione che di fatto non è quella reale. Peraltro risulta a nostro avviso positiva l'indicazione di valutare la riduzione del rischio a fronte di azioni di mitigazione solo ipotizzate, giustificandone così la realizzazione qualora le azioni stesse riducano sensibilmente il rischio.

SEZIONE IV - IL SISTEMA DI GESTIONE DELLA SICUREZZA INFORMATICA

Nessuna osservazione

SEZIONE V - IL SISTEMA DI GESTIONE DEI DATI

La disposizione, così come formulata, prevede un "*sistema di gestione dati*" con livelli omogenei di pervasività, strutturazione e completezza, la cui attuazione comporterebbe, per l'intermediario, investimenti e costi assai rilevanti (infatti per qualunque dato gestito, di qualsivoglia natura operativa o gestionale, su qualsivoglia sistema mainframe, *open*/dipartimentale, di qualunque banca appartenente al Gruppo, dovrebbero essere identificate e documentate le responsabilità, le procedure di gestione, estrazione ed elaborazione, le assunzioni e i criteri, i destinatari,…). Anche per questa disposizione è fortemente auspicabile che siano applicabili criteri di rilevanza, di importanza, di progressività e di rischiosità in modo da orientare strategicamente gli investimenti e costi connessi.

SEZIONE VI – L'ESTRENALIZZAZIONE DI SISTEMI E SERVIZI ICT

1.1 Tipologie di esternalizzazioni

Nessuna osservazione

1.2 Accordo con i fornitori e altri requisiti

Il capitolo 8 sezione VI rimanda, per le disposizioni di carattere generale, a quanto riportato nel capitolo 7 sezione IV (outsourcing).

Per quanto concerne il mantenimento delle "*competenze tecniche e gestionali per re-internalizzare…*" le attività esternalizzate, si rimanda a quanto più volte evidenziato in precedenza, in particolare con riferimento alla differenziazione in caso l'esternalizzazione avvenga su società controllate e/o appartenenti al gruppo bancario dell'intermediario.

In tali casi infatti, pur rimanendo la responsabilità in capo all'intermediario, tanto i meccanismi di governance in essere quanto le modalità e i termini di eventuali re-internalizzazioni, rendono non strettamente necessaria, oltrechè antieconomica, la disposizione.

Infine UniCredit ritiene che possa essere opportuno prevedere che nei contratti con i fornitori di sistemi e servizi ICT vengano specificati i requisiti di *disaster recovery* e di continuità operativa dei servizi e infrastrutture ICT oggetto di fornitura.

1.3 Indicazioni particolari

Nessuna osservazione

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

Nessuna osservazione

ALLEGATO B – MISURE IN MATERIA DI SERVIZI TELEMATICI PER LA CLIENTELA

1.1 Verifica dell'autentica del sito web e cifratura del canale di distribuzione

Nessuna osservazione

1.2 Procedura di autenticazione del cliente

Si chiede di precisare gli ambiti di applicazione della procedura di "*autenticazione forte*" e, in particolare, se la stessa debba essere utilizzata in occasione di ogni accesso dell'utente, ovvero se – al fine di semplificare le attività richieste a quest'ultimo – possa essere limitata alle sole operazioni di carattere dispositivo, con esclusione di quelle meramente informative (ad esempio, consultazione dell'anagrafica, della situazione contabile) che sarebbero gestite mediante codice identificativo e PIN o password.

1.3 Autorizzazione e monitoraggio delle transazioni di pagamento

Nessuna osservazione

1.4 Sensibilizzazione della clientela

Nessuna osservazione

TITOLO V – CAPITOLO 9 DISPOSIZIONI IN MATERIA DI CONTINUITA' OPERATIVA

DISPOSIZIONI IN MATERIA DI CONTINUITA' OPERATIVA

Con riferimento al "*Tempo massimo accettabile di interruzione del servizio*" si ritiene utile, per maggior chiarezza, che venga aggiunta nel paragrafo 3 una definizione specifica che caratterizzi questa grandezza/requisito. Al riguardo si suggerisce: "*Tempo massimo accettabile di interruzione*

del servizio: *tempo oltre il quale gli impatti negativi, che potrebbero verificarsi a causa della mancata erogazione di un prodotto/servizio o svolgimento di una attività, diventa inaccettabile*"[3].

Con riferimento alla correlazione dei rischi, si propone di modificare quanto riportato nel paragrafo 5 come segue: "*i rischi residui non gestiti dal piano rientrano nelle valutazioni delle componenti di alcune metriche del risk appetite/risk tolerance (componente di assorbimento di capitale da "rischio operativo PILLAR 1 – Advanced Measurement Approach - AMA) e sono documentati e esplicitamente accettati dall'intermediario.*"

Infine, in merito ai tempi di ripristino e percentuali di disponibilità, si suggerisce di integrare la seguente previsione normativa come di seguito:

Il tempo di ripristino dei processi a rilevanza sistemica in caso di incidente è contenuto:
a) per banche e gruppi bancari: entro 4 ore dal momento dell'interruzione del servizio;
b) per sistemi di pagamento e relativi fornitori di servizi tecnologici: entro 2 ore dal momento dell'interruzione del servizio.

Infine nel paragrafo 7.5 si suggerisce di modificare il punto "*Nel caso in cui il disastro comporti un blocco dei servizi essenziali ovvero si registri una situazione di gravi danni o di serio pericolo sul lato umano, è possibile che gli obiettivi sopra enunciati subiscano un adattamento, in via straordinaria, sulla base delle indicazioni fissate nelle sedi nazionali di coordinamento della crisi*" con la seguente formulazione: "*Nel caso in cui il disastro comporti un blocco dei servizi essenziali ovvero si registri una situazione di gravi danni o di serio pericolo sul lato umano anche di uno solo dei soggetti ai quali si applicano i requisiti particolari per la continuità operativa, è possibile che gli obiettivi sopra enunciati subiscano un adattamento, in via straordinaria, sulla base delle indicazioni fissate nelle sedi nazionali e di settore di coordinamento della crisi*".

Tale modifica, propone un parametro quantitativo e misurabile. Tuttavia tale parametro può essere mitigato secondo un aspetto più qualitativo che il singolo operatore in casi di grave difficoltà può negoziare direttamente con Banca d'Italia.

3 In linea con la definizione del "Maximum acceptable outage – MAO" contenuta nello standard ISO22301 – 2012.