UBI Banca

Considerazioni UBI Banca sul documento per la consultazione di Banca d'Italia: "Disposizioni di vigilanza prudenziale per le Banche - Sistema dei Controlli Interni, Sistema Informativo e Continuità Operativa"

Ottobre 2012

UBI Banca ringrazia la Banca d'Italia per la consultazione sulle "Disposizioni di vigilanza prudenziale per le Banche - Sistema dei Controlli Interni, Sistema Informativo e Continuità Operativa" che si inseriranno nella circolare n. 263 del 27 dicembre 2006, "Nuove disposizioni di vigilanza prudenziale per le banche", in sostituzione della parte riguardante "La gestione e il controllo dei rischi. Ruolo degli organi aziendali".

Il documento rappresenta la sintesi dei commenti e delle proposte di UBI Banca sui vari argomenti trattati nel documento in consultazione con particolare attenzione ai seguenti aspetti:

1) Questioni specifiche evidenziate nei 5 box individuati dalla Banca d'Italia a pag. vii del documento in consultazione;
2) L'istituzione e i compiti delle funzioni aziendali di controllo;
3) L'esternalizzazione di funzioni aziendali;
4) I controlli nei gruppi bancari;
5) Il sistema informativo.

Sono riportate in corsivo le principali previsioni della Disposizioni oggetto di commento.

In linea generale si evidenzia l'opportunità di indicare nel documento definitivo la data di entrata in vigore della nuova disciplina.

1. Questioni specifiche evidenziate nei 5 box individuati dalla Banca d'Italia

BOX 1 :

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

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.

***Osservazioni, commenti e proposte*:**

Si condivide l'utilizzo di variabili di natura sia quantitativa che qualitativa per la determinazione della tolleranza al rischio, che già oggi viene declinata, a livello consolidato, con riferimento ad esempio a:

- Solidità patrimoniale - espressa sia in termini di misure regolamentari (core tier I ratio) sia interne (rapporto tra risorse finanziarie disponibili – AFR – e capitale interno complessivo);
- Equilibrio finanziario, espresso sia in termini di corretto equilibrio tra le fonti e gli impieghi (NSFR), sia di adeguate riserve liquide per fronteggiare situazioni di crisi (LCR);
- Creazione di valore (EVA);
- Valutazione del posizionamento sul mercato, basato sulla determinazione del rating target tendenziale;
- Assetto organizzativo-informatico e dei controlli, basato sulla minimizzazione dei possibili impatti derivanti dai rischi perseguibile attraverso l'adozione di policy a presidio dei rischi, rigorosi presidi organizzativi, metodologie di misurazione e strumenti di mitigazione.

Coerentemente con i target complessivi di propensione al rischio viene declinato, per i rischi misurabili, il capitale allocato. Sulla base del capitale allocato sono definiti a cascata i limiti operativi.

BOX 2:

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

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

***Osservazioni, commenti e proposte*:**

In coerenza con l'approccio seguito per la definizione della tolleranza al rischio, si ritiene opportuno lasciare all'autonomia delle singole Banche la determinazione delle modalità di individuazione delle operazioni rilevanti.

La definizione di soglie normative deterministiche, funzionali all'identificazione delle operazioni di maggior rilievo, potrebbe esporre alle seguenti controindicazioni:

- Le dimensioni di analisi e le relative soglie sarebbero difficilmente determinabili in modo uniforme con riferimento a tutti i destinatari della normativa, quantomeno a causa delle peculiarità di composizione dei portafogli di clientela di ciascuna realtà destinataria (es. portafoglio locale vs a caratterizzazione estera; portafoglio prevalentemente retail vs corporate, etc.);
- L'utilizzo del concetto di rilevanza in termini deterministici rischierebbe di confinare sistematicamente nell'area di irrilevanza alcune categorie di operazioni caratterizzate dalla preponderanza di rischiosità non facilmente misurabile (es. operazioni che espongono a rischio reputazionale).

BOX 3

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

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.

***Osservazioni, commenti e proposte*:**

Non si ritiene opportuno declinare ulteriori elementi caratterizzanti il principio di proporzionalità, rispetto a quelli già evincibili dalla normativa vigente (es. macro-categorie individuate a fini SREP).

BOX 4:

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

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

***Osservazioni, commenti e proposte*:**

Si considera a tutti gli effetti il rischio informatico come un sottoinsieme molto importante dei rischi operativi. Cio' nonostante per motivi di coerenza complessiva non se ne prevede un trattamento ad hoc se non all'interno della gestione dei rischi operativi. Resta confermata la necessità di garantire una adeguata comprensione a tutti i livelli di questa tipologia di rischio come esplicitamente raccomandato nel documento in consultazione.

BOX 5:

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

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

***Osservazioni, commenti e proposte*:**

Pur comprendendo le importanti implicazioni derivanti dalla soluzione in oggetto si ritiene indispensabile attendere un periodo adeguato di operatività che consenta di apprezzare fino in fondo le implicazioni sulla sicurezza di una soluzione che di fatto esternalizza la collocazione di dati sensibili.

2. Funzioni aziendali di controllo (Capitolo 7, Sezione III)

Capitolo 7, Sezione III (paragrafo 1, paragrafo 3.2)

Le funzioni aziendali di controllo permanenti e indipendenti sono tre: i) di conformità alle norme; ii) di controllo dei rischi; iii) di revisione interna. Le prime due funzioni attengono ai controlli di secondo livello.

I responsabili siano collocati in posizione gerarchico funzionale adeguata, non abbiano responsabilità diretta di aree operative sottoposte a controllo nè siano gerarchicamente subordinati ai responsabili di tali aree; riferiscano direttamente agli organi aziendali. Le funzioni aziendali di controllo siano tra loro separate, sotto un profilo organizzativo. Se coerente con il

principio di proporzionalità e a condizione che i controlli continuino ad essere efficaci le banche possono affidare la funzione di conformità alle strutture incaricate del controllo dei rischi.

In tema di requisiti specifici delle varie funzioni di controllo con riferimento alla funzione di conformità viene evidenziato che la stessa presiede alla gestione del rischio di non conformità alle norme, con riguardo a tutta l'attività aziendale. Particolare attenzione deve essere posta anche nella verifica della conformità alle normative di natura fiscale incluse quelle poste in essere dalla clientela da cui potrebbe derivare un coinvolgimento della banca.

***Osservazioni, commenti e proposte*:**

Al riguardo si ritiene opportuno chiarire, al fine di evitare incertezze applicative della disciplina, la distinzione tra attribuzioni assegnate alle funzioni di controllo rispetto alle soluzioni organizzative (strutture/unità organizzative) più idonee a consentire un efficace presidio sui rischi e per le quali dalla lettura del documento in consultazione, sembrerebbe sia riconosciuta alle banche un grado di flessibilità, in relazione alle caratteristiche dell'intermediario e a condizione di una piena trasparenza sulle scelte effettuate e nel rispetto degli obiettivi sostanziali della normativa.

Considerando quanto riportato nella nota del Governatore di Banca d'Italia per l'applicazione delle disposizioni di vigilanza in materia di organizzazione e governo societario delle banche, che invitava a porre attenzione sul "corretto ed efficiente funzionamento della funzione di gestione del rischio (*risk management*) […] nonché sul soggetto responsabile di tale funzione (*chief risk officer*)", e tenuto conto della relazione preliminare che accompagna il documento in consultazione (laddove viene citato il CRO nell'ambito della funzione di controllo dei rischi) nonché dei contributi sul tema prodotti dalle diverse istituzioni internazionali competenti (es. Principio n°6 di "*Principles for enhancing corporate governance*" del Comitato di Basilea), si ritiene che la funzione di controllo dei rischi (risk management function) sia di responsabilità del CRO, laddove istituito. Si auspica una esplicita indicazione in tal senso nel documento in consultazione.

La distinzione tra funzione e unità organizzativa sopra richiamata consente di affermare che l'attribuzione della funzione di conformità alle norme (compliance) al responsabile dell'unità che si occupa della gestione dei rischi di conformità non pone vincoli di carattere organizzativo, anche qualora tale soggetto riporti gerarchicamente al CRO, purché il responsabile di detta funzione mantenga la possibilità, come già avviene sulla base della normativa attualmente vigente, di comunicare agli Organi di Amministrazione e Controllo in via indipendente, mediante invio di flussi informativi e con partecipazione diretta, se richiesta.

L'interpretazione della disciplina è che la funzione di Compliance debba presidiare tutte le normative, utilizzando a livello organizzativo un approccio di tipo matriciale, nel quale sono definiti puntualmente i livelli di responsabilità diretta (es. Mifid, Trasparenza, ecc..) ovvero indiretta (es. Antiriciclaggio, Fiscale, ecc..); per questi ultimi la verifica dei relativi profili di conformità può essere attribuita alle strutture caratterizzate da maggiore specializzazione nell'ambito di riferimento purchè i presidi dedicati a tematiche ad elevato contenuto specialistico garantiscano alla Compliance le necessarie attestazioni rispetto all'attività svolta. In coerenza con tale approccio, relativamente all'ambito fiscale, richiamato nel documento in consultazione, si ritiene che la Compliance debba contribuire alla definizione del framework normativo interno con riguardo in particolare all'attività di consulenza fiscale verso la clientela. L'approccio, comunque finalizzato ad una corretta gestione dei rischi, anche di tipo reputazionale, è volto ad evitare che alla Compliance siano attribuite responsabilità dirette su ambiti che richiederebbero duplicazioni di competenze e strutture. Più in generale, si osserva che quest'ultimo aspetto è ampiamente evidenziato anche al paragrafo 5 sul coordinamento delle funzioni di controllo interne ed esterne (sezione II, par.5)… *"Il*

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

Al riguardo si richiama l'attenzione sull'opportunità di chiarire che l'ambito della circ. 263 di Banca d'Italia (laddove non già ampiamente esplicitato come nel Titolo V- Capitolo 4 e 5), su cui permangono incertezze applicative della disciplina in termini di responsabilità sulle verifiche di conformità e su cui a volte questa funzione è chiamata in causa direttamente (es. Segnalazioni, CRM), rientri indirettamente nel perimetro della funzione di conformità in coerenza con quanto precedentemente esposto. Per il presidio di tale normativa, nell'organizzazione attuale della Banca, sono già operative strutture che si occupano di tali ambiti e in attuazione della nuova disciplina potrebbe essere previsto, anche in questo caso, che le strutture garantiscano alla Compliance flussi informativi adeguati e corrispondenti attestazioni per i controlli svolti, secondo il principio della responsabilità indiretta anziché diretta di conformità alle norme. A titolo di esempio, in ambito Credit Risk Mitigation, la Compliance potrebbe contribuire a definire l'insieme dei controlli attesi per quanto previsto dalla normativa, al fine di alimentare una matrice delle verifiche di conformità uniforme a livello di Gruppo.

Secondo tale interpretazione (approccio matriciale, responsabilità diretta e indiretta della Compliance), che si ritiene debba essere maggiormente esplicitata nel documento in consultazione, le attribuzioni attese della funzione di conformità richiedono che la stessa abbia comunque contezza dell'esistenza e del funzionamento di processi e procedure anche per gli ambiti non di diretta competenza, al fine di garantire agli organi aziendali il quadro complessivo sull'adeguatezza della conformità alle norme.

Capitolo 7, Sezione III (paragrafo 3.3)

Al fine di rafforzarne l'indipendenza, il responsabile della funzione di controllo dei rischi puo' essere collocato alle dirette dipendenze del comitato controllo e rischi, ove costituito, o dell'organo con funzione di supervisione strategica. Viene poi espressamente richiesto nella nota 22 di pagina 19, *nel caso di Banche classificate ai fini SREP nelle macro-categorie 1 e 2 un suo collocamento obbligatorio alle dirette dipendenze del comitato controllo e rischi, ove costituito o dell'organo con funzione di supervisione strategica.*

In tema di partecipazione della funzione ai comitati di gestione dei diversi profili di rischio (ad es. comitati per i rischi di credito e operativi, comitato di liquidità, ecc..) viene chiesto di *"…definire in modo chiaro le diverse responsabilità e le modalità di intervento e di partecipazione della funzione in modo da garantirne la completa indipendenza dal processo di assunzione dei rischi; va inoltre evitato che l'istituzione di tali comitati possa depotenziare le prerogative della funzione di controllo dei rischi.*

Al tempo stesso, vanno individuate soluzioni organizzative che non determino una eccessiva distanza dal contesto operativo. Per la piena consapevolezza dei rischi è necessario che vi sia una continua interazione critica con le unità di business.

***Osservazioni, commenti e proposte*:**

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

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

Tenendo fermo il principio in precedenza esposto per la Compliance di distinzione tra funzione e unità/struttura organizzativa, anche l'attribuzione della funzione di gestione dei rischi al Chief Risk Officer non pone vincoli di carattere organizzativo, anche qualora questi, come nel Gruppo UBI, riporti gerarchicamente al Chief Executive Officer (Consigliere Delegato, responsabile di promuovere il presidio integrato dei rischi), e sia formalizzato che il responsabile di detta funzione mantenga la possibilità di comunicare agli organi di Amministrazione e Controllo in via indipendente, mediante invio di flussi informativi e con partecipazione diretta, sia in maniera regolare che su richiesta.

Questa interpretazione inoltre, renderebbe più lineare la coerenza tra la funzioni di controllo di terzo livello (Audit) che riporta direttamente all'organo con funzione di supervisione strategica e di controllo (Consiglio di Sorveglianza nel caso UBI Banca) e la funzione di controllo di secondo livello (CRO) in riporto gerarchico al CEO, evitando quindi possibili duplicazioni e sovrapposizioni di ruolo tra le due.

Ad ulteriore evidenza del grado di indipendenza del CRO rispetto al CEO sono le procedure di nomina/revoca e di remunerazione dei responsabili delle funzioni di controllo e quindi anche del CRO che non rientrano nelle autonome attribuzioni del CEO ma di comitati indipendenti costituiti in seno al Consiglio di Sorveglianza.

Da ultimo si consideri che tale interpretazione, non irrigidirebbe le modalità di funzionamento degli organi aziendali e delle funzioni di controllo interne e societarie previsti dalla nuova disciplina

(Capitolo 7-Sezione II), attenuando il rischio di applicazioni nel caso concreto, molto onerose ed eterogenee ad esempio tra banche che adottano un sistema di amministrazione e controllo di tipo dualistico anziché tradizionale (basato sul Consiglio di Amministrazione e Collegio Sindacale e ispiratore del modello di corporate governante delineato nel Codice di Autodisciplina a cui il documento in consultazione si ispira) che di fatto potrebbero dimostrarsi formalmente rispettose delle previsioni normative ma meno efficaci nell'applicazione dei principi generali alla base della disciplina che mirerebbe a promuovere il rafforzamento della capacità di gestire e prevenire i rischi a rinforzo della sana e prudente gestione delle banche e della stabilità del sistema finanziario.

In relazione a quanto sopra riferito si auspica una riformulazione della nota 22 di pag. 19.

Capitolo 7, Sezione III (paragrafo 3.5)

Specifica attenzione è posta nell'articolazione dei flussi informativi tra le funzioni aziendali di controllo; in particolare il responsabile della revisione interna informa i responsabili delle altre funzioni aziendali di controllo per le eventuali inefficienze, punti di debolezza o irregolarità emerse nel corso delle attività di verifica di propria competenza e riguardanti specifiche aree o materie di competenza di queste ultime.

***Osservazioni, commenti e proposte*:**

L'"*articolazione dei flussi informativi tra le funzioni aziendali di controllo"* è specificamente disciplinata nelle disposizioni inerenti: i) la funzione di conformità alla norme (Capitolo 7, Sezione III, Paragrafo 3. 2 - pag. 17) laddove prevede *la predisposizione di flussi informativi diretti agli organi aziendali e alle strutture coinvolte (es.: gestione del rischio operativo e revisione interna; ii)* la funzione di internal audit nell'ambito dei rapporti fra le funzioni aziendali di controllo e le altre funzioni aziendali sopra riportate (Capitolo 7, Sezione III, Paragrafo 3. 5 - pag. 22). Analogamente sarebbe auspicabile che nelle previsioni concernenti la funzione di controllo dei rischi (Capitolo 7, Sezione III, Paragrafo 3. 3 - pag. 19) fosse espressamente disciplinata la materia.

Allegato A- Disposizioni speciali relative a particolari categorie di rischio (pag.36)

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

Allegato B – Controlli sulle succursali estere (pag. 42)

….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 auspica siano individuati, anche a titolo esemplificativo similmente a quanto rappresentato in altri ambiti del documento, criteri qualitativi e quantitativi sulla base dei quali individuare l'*"operatività significativa".* Al riguardo potrebbero essere valutati quale riferimento aspetti inerenti le autonomie deliberative, la tipologia dei prodotti commercializzati, la legislazione locale di riferimento.

3. Esternalizzazione di funzioni aziendali (Capitolo 7, Sezione IV)

Capitolo 7, Sezione IV, Paragrafo 1 (pag.23 e 24)

La decisione di ricorrere all'outsourcing per lo svolgimento di determinate funzioni aziendali deve essere coerente con la politica aziendale in materia di esternalizzazione approvata dall'organo con funzione di supervisione strategica. Le banche che ricorrono all'esternalizzazione di funzioni aziendali devono presidiare i rischi derivanti dalle scelte effettuate, mantenendo la capacità di controllo e la responsabilità sulle attività esternalizzate nonché le competenze tecniche e gestionali essenziali per re-internalizzare, in caso di necessità, il loro svolgimento.

la banca:
a) conserva la competenza richiesta per controllare efficacemente le funzioni esternalizzate e per gestire i rischi connessi con l'esternalizzazione, inclusi quelli derivanti da potenziali conflitti di 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").

***Osservazioni, commenti e proposte*:**

Nell'interpretazione della disciplina è chiara e condivisibile la finalità di istituire forti presidi nelle singole entità del Gruppo per le attività/servizi esternalizzati. Al riguardo si ritiene opportuno un chiarimento in merito alle modalità di collegamento tra questo paragrafo e quanto successivamente previsto in tema di sistema dei controlli nei gruppi bancari nel caso di outsourcing interno ad un Gruppo bancario. In particolare, ci si riferisce alle indicazioni previste nella Sezione V paragrafo 2: *….vanno anche stabiliti e definiti: procedure formalizzate di coordinamento e collegamento fra le società appartenenti al gruppo e la capogruppo per tutte le aree di attività;….. meccanismi di integrazione dei sistemi informativi e dei processi di gestione dei dati anche al fine di garantire l'affidabilità delle rilevazioni su base consolidata; procedure che garantiscano a livello accentrato un efficace processo di gestione dei rischi a livello consolidato con particolare attenzione all'anagrafe unica o di piu' anagrafi raccordabili in modo da consentire l'univoca identificazione da parte delle diverse entità dei singoli clienti…..* da cui discenderebbe la possibilità in capo agli organi aziendali della Capogruppo di definire il livello più adeguato di accentramento delle proprie aree di attività, purchè siano garantiti adeguati flussi informativi, sia individuato un responsabile del controllo delle funzioni esternalizzate ("referente per le attività esternalizzate"), meccanismi di coordinamento e controllo nel rispetto dei principi generali della disciplina (e nel caso di esternalizzazione delle funzioni di controllo presso la capogruppo delle condizioni previste dalla

disciplina alla Sezione V par. 2 pag. 28) e nel caso di funzioni operative importanti o di controllo sia stata ottenuta l'autorizzazione preventiva di Banca d'Italia.

La previsione di mantenere "*le competenze tecniche e gestionali essenziali per re-internalizzare, in caso di necessità, il loro svolgimento"* qualora interpretata in senso letterale comporterebbe nel caso di outsourcing interno, l'istituzione presso le singole entità appartenenti al Gruppo Bancario di autonome strutture con duplicazioni di competenze in certi casi molto scarse.

4. Sistema dei Controlli nei gruppi bancari (Capitolo 7, Sezione V)

Capitolo 7, Sezione V, Paragrafo II (pag. 28)

L'esternalizzazione delle funzioni di controllo presso la capogruppo è consentita a condizione che:……all'interno di tutte le banche e entità che assumono rischi considerati rilevanti vengono individuati appositi referenti i quali svolgono compiti di supporto per la funzione aziendale di controllo esternalizzata; riportano funzionalmente e gerarchicamente a quest'ultima; provvedono tempestivamente a segnalare eventi o situazioni particolari, suscettibili di modificare i rischi generati dalla controllata. Nota 26: A seconda della funzione aziendale di controllo esternalizzata può trattarsi di responsabili di unità di controllo del rischio locali, "compliance officer", responsabili di unità distaccate di internal audit.

***Osservazioni, commenti e proposte*:**

In relazione ai compiti ed alle attribuzioni della figura di "referente per le attività esternalizzazione di auditing" citata al punto precedente sull'esternalizzazione di funzioni aziendali (Sezione IV, Paragrafo 1, pag. 24), fra cui in particolare il supporto al consiglio di amministrazione nella valutazione dei rischi emersi dalle attività di internal auditing e degli interventi proposti a mitigazione degli stessi, nonché nella valutazione del rispetto delle previsioni contrattuali anche con specifico riguardo ai livelli di servizio concordati con l'outsoucer – detta figura potrebbe essere individuata in un consigliere indipendente ovvero nel comitato controllo e rischi. Tale soluzione organizzativa, che appare coerente con le previsioni in tema di indipendenza ed autonomia della funzione di revisione interna, prevede la formalizzazione di idonei flussi informativi e meccanismi di comunicazione aventi caratteristiche di periodicità e contenuto funzionali all'esercizio del ruolo.

Inoltre, coerentemente con quanto previsto al paragrafo II pag. 28, con compiti di supporto della funzione di Internal Audit esternalizzata presso la Capogruppo sono individuati appositi referenti, che riportano funzionalmente e gerarchicamente alla struttura di revisione interna di Capogruppo, responsabili di unità distaccate di internal audit nelle singole Controllate. Dette unità distaccate svolgono l'attività di internal auditing su base individuale per ciascuna Controllata in linea con la separatezza richiesta rispetto alle unità e risorse deputate ai controlli su base consolidata.

Nel caso delle altre funzioni di controllo di secondo livello, in virtu' del grado di flessibilità riconosciuto alle Banche rispetto alle soluzioni organizzative piu' idonee a consentire un efficace presidio sui rischi, e della responsabilità in capo alle singole entità del gruppo sulle attività esternalizzate, si ritiene opportuno riconoscere un maggior grado di flessibilità consentendo che il referente con compiti di supporto riporti funzionalmente, ma non necessariamente anche gerarchicamente alla funzione di controllo di capogruppo.

Capitolo 7, Sezione V, Paragrafo II (pag. 29)

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

***Osservazioni, commenti e proposte*:**

La previsione di mantenere "*un'adeguata separazione tra le unità e le risorse deputate a svolgere l'internal audit su base individuale per le controllate da quelle responsabili dei controlli su base consolidata",* qualora interpretata in senso restrittivo comporterebbe l'istituzione all'interno della funzione di revisione della capogruppo di autonome strutture di audit con duplicazioni di skill e risorse dedicate.

5. Sistema Informativo (Capitolo 8, Sezione II e III)

Governo e Organizzazione dell'ICT

Capitolo 8, Sezione II, Paragrafo 1, 2 (pag. 47-48)

L'organo con funzione di supervisione strategica ha compiti ben precisi in tema di delibera dell'architettura dei sistemi informativi, delle linee di indirizzo in materia di approvvigionamento delle risorse (modalità di assunzione del personale, di acquisizione dei sistemi, software e servizi incluso in ricorso a fornitori esterni), approva il quadro di riferimento organizzativo e metodologico per l'analisi del rischio informatico per assicurare che tale categoria di rischio sia regolarmente identificata,valutata e rendicontata, approva il livello di tolleranza del rischio informatico, è informato con cadenza almeno annuale sulla situazione di rischio informatico rispetto al livello accettato di tolleranza.

L'organo con funzione di gestione definisce l'organigramma della funzione ICT, disegna e segue l'implementazione dei processi di gestione dell'ICT incluso il processo di analisi del rischio informatico, approva gli standard di data governance, le procedure di gestione dei cambiamenti e degli incidenti, il piano operativo, fornisce un rapporto sintetico su valore e costi dell'ICT e con periodicità almeno annuale fornisce all'organo con funzione di supervisione strategica flussi informativi sulla situazione del rischio tecnologico.

Nell'allegato A, vengono riportati i documenti che l'organo con funzione di supervisione strategica e l'organo con funzione di gestione devono approvare nell'ambito dei rispettivi ruoli e responsabilità nella materia.

***Osservazioni, commenti e proposte*:**

Nell'interpretazione della disciplina sopra richiamata e coerentemente con quanto definito nel Capitolo 7, Sezione II sul ruolo della funzione di supervisione strategica e di gestione (Consiglio di Sorveglianza e di Gestione per UBI) in ambito di approvazione, definizione e attuazione della politica aziendale in materia di esternalizzazione di funzioni aziendali, nel caso in cui la gestione dell'ICT sia data in outsourcing ad una società di servizi interna al Gruppo Bancario, si ritiene corretta l'interpretazione che prevede l'approvazione dei documenti riportati nell'Allegato A da parte degli Organi di Amministrazione e Controllo della società di servizi interna con una successiva approvazione da parte del Consiglio di Sorveglianza e di Gestione della Capogruppo e delle altre Banche/Società affinchè le stesse siano consapevoli delle scelte effettuate, purchè siano previsti adeguati flussi informativi e meccanismi di coordinamento con i referenti per le attività

esternalizzate individuati presso le varie entità del Gruppo (Capogruppo inclusa) a garanzia della capacità della singola realtà di valutare e gestire i rischi conseguenti alle scelte gestionali in ambito ICT effettuate dalla società di servizi su mandato della Capogruppo. Si ricorda inoltre che nel caso di presenza di soluzioni societarie consortili è previsto che in sede consigliare e/o assembleare sia data adeguata rappresentazione delle strategie e dei progetti di rilevanza strategica previsti e in corso di attuazione.

Capitolo 8, Sezione II, Paragrafo 3 (pag. 49)

E' richiesta nelle realtà piu' complesse la previsione di un organo (direttore dei sistemi informativi o equivalente) che assuma la generale responsabilità della funzione con riporto diretto verso l'organo con funzione di gestione a garanzia dell'unitarietà della visione gestionale e del rischio informatico nonché dell'uniformità di applicazione delle norme riguardanti i sistemi informativi.

***Osservazioni, commenti e proposte*:**

Come per il punto precedente nel caso di ICT in outsourcing interno al Gruppo Bancario si ritiene corretta l'interpretazione che prevede l'attribuzione del ruolo di direttore dei sistemi informativi al Direttore Generale della società interna di servizi come figura responsabile *super partes* che riconduce ad unitarieta' le diverse componenti dei sistemi informativi del Gruppo che risponde direttamente all'organo di Amministrazione e Controllo della stessa ed indirettamente al Consiglio di Gestione della Capogruppo per il tramite della figura interna alla Capogruppo di Chief Operating Officer.

La gestione del rischio informatico

Capitolo 8, Sezione III (pag. 50)

Il processo di analisi del rischio informatico deve essere svolto dall'utente responsabile con la partecipazione del personale tecnico, secondo una metodologia definita dall'organo con funzione di gestione.

***Osservazioni, commenti e proposte*:**

In tema di processi di analisi e di valutazione su base periodica del rischio informatico (definito chiaramente dalla normativa come di cui dei rischi operativi) si richiama l'attenzione sull'opportunità di prevedere un quadro normativo che fornisca chiare indicazioni sulle possibilità e modalità di sinergie con le metodologie di valutazione attualmente in uso per i rischi operativi da parte dei Gruppi Bancari autorizzati all'adozione di metodi Avanzati (AMA).

Al riguardo, sarebbe opportuno chiarire, al fine di evitare incertezze applicative della disciplina, la natura della nuova figura di utente responsabile identificata dalla normativa e che sembrerebbe essere riconducibile ad un ruolo di system owner. Tale "system owner" è definito dalla disciplina come "*la figura aziendale identificata per ciascun sistema che ne assume la generale responsabilità amministrativa in rappresentanza degli utenti, in rapporto con le funzioni preposte allo sviluppo e alla gestione tecnica*" e sembrerebbe corrispondere alla figura aziendale preposta alla certificazione del dato trattato informaticamente dalla procedura di riferimento e quindi esterna alla struttura di sviluppo ICT e più vicino ad una figura di business/control owner funzionalmente competente, che per molte realtà soprattutto in Italia, sarebbe da identificare.