BNL
GRUPPO BNP PARIBAS

Direzione Compliance
Rischi Operativi e Coordinamento Controlli Permanenti
Via di Santa Prisca, 26
00153 Roma

Spett. le
Banca d'Italia
Divisione Normativa Prudenziale
Servizio Normative e Politiche di Vigilanza

Via Milano, 53
00184 Roma

Roma, 31 ottobre 2012

Oggetto: Documento per la consultazione – Disposizioni di Vigilanza Prudenziale per le Banche. Controlli Interni, Sistema Informativo e Continuità Operativa

Si ringrazia codesta Autorità per aver coinvolto gli intermediari nella valutazione dei contenuti del documento in oggetto.

Con l'auspicio che sia assicurato un congruo tempo di adeguamento, si trasmettono in allegato i commenti e le proposte di BNL S.p.A.

Si coglie l'occasione per porgere i migliori saluti.

BNL SpA – Direzione Generale
C. Incagnoli G. Crescenti

DOCUMENTO PER LA CONSULTAZIONE
DISPOSIZIONI DI VIGILANZA PRUDENZIALE PER LE BANCHE
SISTEMA DEI CONTROLLI INTERNI, SISTEMA INFORMATIVO E CONTINUITA' OPERATIVA

Di seguito i commenti e le eventuali proposte di revisione/integrazione della normativa oggetto di consultazione.

TITOLO V - CAPITOLO VII - Il Sistema dei Controlli Interni

❖ Sezione I, par. 6 - Principi generali

[...] A prescindere dalle strutture dove sono collocate, si possono individuare le seguenti tipologie di controllo:
[...] Controlli di linea (c.d. "controlli di primo livello), diretti ad assicurare il corretto svolgimento delle operazioni. Essi sono effettuati dalle stesse strutture operative (es. controlli di tipo gerarchico, sistematici e a campione), anche attraverso diverse unità che riportano ai responsabili delle strutture operative, ovvero eseguiti nell'ambito del back office; per quanto possibile, essi sono incorporati nelle procedure informatiche. Le strutture operative sono le prime responsabili del processo di gestione dei rischi: nel corso dell'operatività giornaliera tali strutture devono identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale in conformità con il processo di gestione dei rischi; esse devono assicurare il rispetto del livello di tolleranza al rischio stabilito e delle procedure in cui si articola il processo di gestione dei rischi; [...]
[...] Revisione interna (c.d. "controlli di terzo livello"), volta ad individuare ***andamenti anomali, violazione delle procedure e della regolamentazione*** *nonché a valutare periodicamente la completezza, la funzionalità e l'adeguatezza, in termini di efficienza ed efficacia, del sistema dei controlli interni, inclusi quelli sul sistema informativo (ICT audit), con cadenza prefissata in relazione alla natura e all'intensità dei rischi. [...]*

Con specifico riferimento alla previsione relativa ai controlli di linea, si propone di inserire dopo la frase:

- *"per quanto possibile, essi sono incorporati nelle procedure informatiche"*

la seguente:

- *"Con riferimento alle realtà operative più complesse possono essere previste unità dedicate ai controlli di primo livello non coinvolte nell'operatività e che rappresentano un primo presidio in quanto svolgono controlli volti a verificare e misurare la conformità dell'operatività alle norme e l'efficienza/efficacia dei processi [...]."*

L'integrazione si rende opportuna con particolare riferimento ai controlli sui rischi operativi che, per essere efficaci, richiedono per il loro svolgimento professionalità specifiche e quindi ruoli specializzati per tipologia di operatività anche al primo livello.

Con specifico riferimento alle seguenti due previsioni relative alla revisione interna:

- *"[...]* ***revisione interna*** *(c.d. "controlli di terzo livello"), volta ad individuare [...]* ***violazione delle procedure e della regolamentazione*** *[...]".*
- *"la funzione di revisione interna* ***espleta compiti d'accertamento anche con riguardo a specifiche irregolarità****, ove richiesto dagli organi aziendali"*[1]*,*

[1] Sezione III – par. 3 Requisiti specifici delle funzioni aziendali di controllo. 3.4 Funzione di revisione interna.

si propone di valutare se diffondere in capo ai diversi livelli di funzione di controllo tali obblighi (dunque anche ma non solo in capo alla revisione interna), per escludere che vi si legga una sorta di riserva di attività in capo alla revisione interna.
Anche a promozione della rilevanza della cultura del controllo statuita alla Sezione I. Paragrafo 6. Principi Generali, si propone dunque di eliminare le specifiche previsioni nei brani puntualmente riferiti alla revisione interna e di integrare come segue la Sezione I. Paragrafo 6. Principi Generali, Pagina 5, 3°cpv.:

- *"Per poter realizzare questo obiettivo, il sistema dei controlli interni deve in generale:*
- *(...)individuare violazioni delle procedure e della regolamentazione ed accertare specifiche irregolarità".*

Con specifico riferimento alla previsione relativa alla revisione interna:

"[...] ***revisione interna*** *(c.d. "controlli di terzo livello"), volta ad individuare* ***andamenti anomali*** *[...]*

Il documento riprende il concetto già espresso nell'ambito della definizione originata nel 1998, attualmente in vigore (Istruzioni di Vigilanza per le Banche – Titolo IV – Capitolo 11 sezione II) relativamente all'*individuazione* degli andamenti anomali.
L'individuazione degli andamenti anomali presuppone tuttavia una sorta di "monitoraggio" dell'operatività che dovrebbe esulare dalla logica del puro controllo *periodico*, tipico dell'internal audit, e che in effetti in altre parti il documento stesso oggi nella sostanza attribuisce a funzioni di controllo di secondo livello[2], tipicamente interessate a presidi di natura *permanente*.
Nondimeno detti andamenti anomali potrebbero restare un fattore di orientamento anche delle attività di revisione interna in virtù di quei flussi informativi tra funzioni di controllo di cui lo stesso documento richiede la definizione.
Dunque si propone di eliminare la locuzione "*a individuare andamenti anomali*".

❖ Sezione II, par. 2 - Determinazione della tolleranza al rischio / appetito per il rischio)

BOX 1

La tolleranza al rischio (risk tollerance) 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*** *coerentemente utilizzate o in via di sviluppo per addivenire a tale determinazione.*

Gli **elementi qualitativi** utilizzati soprattutto per i rischi non misurabili o non facilmente misurabili o per rivedere le politiche chiave e definire più esplicitamente il framework di risk tollerance, sono contenuti sostanzialmente nelle Policy che disciplinano e guidano la gestione dei rischi insiti nei processi.

---

[2] Sezione III – par. 3. Requisiti specifici delle funzioni aziendali di controllo. 3.2 Funzione di conformità alle norme (Compliance): "... individuazione di idonee procedure per la prevenzione del rischio rilevato con possibilità di richiederne l'adozione".
Sezione III – par. 3. Requisiti specifici delle funzioni aziendali di controllo. 3.3 Funzione di controllo dei rischi (Risk management function): "... sviluppa indicatori in grado di evidenziare situazioni di anomalia e di inefficienza dei sistemi di misurazione e controllo dei rischi".

Con riferimento in particolare al rischio di non conformità e di reputazione, si possono utilizzare: il prezzo delle azioni, il rating assegnato all'azienda e al suo marchio (cfr. Fortune), la capacità dell'azienda di attrarre le migliori professionalità e di essere considerata un valido posto per poter crescere professionalmente (vedasi classifiche ad es. "best place to work"). Inoltre sono da considerarsi, in termini di vulnerabilità dell'azienda al manifestarsi del rischio, tutte le iniziative di formazione/informazione volte a diffondere e ad accrescere la cd. "cultura delle conformità", tenendo conto degli orientamenti di business assunti dall'azienda.
Come metodologia di valutazione qualitativa si può assegnare un punteggio (valore alto, medio o basso) in funzione della probabilità dell'accadimento dell'evento dannoso (violazioni con sanzioni penali o con sanzioni amministrative rilevanti, violazioni con sanzioni di più lieve entità, comportamenti non conformi alle sole normative di autoregolamentazione) e dell'impatto potenziale, considerando anche l'effettiva vulnerabilità dell'azienda al rischio analizzato.

Gli **elementi quantitativi** utilizzati per la misurazione della risk tollerance possono essere:

- gli indicatori di performance (KPI), di rischio KRI e di controllo (KCI)
- soglie di allerta in funzione della tipologia di evento che può generare il rischio;
- l'utilizzo delle analisi di scenario in Entità che utilizzano la metodologia AMA;
- le sanzioni comminate all'azienda dalle Autorità di Vigilanza e dagli organismi stragiudiziali.

Con riferimento al ruolo "dell'organo con funzione di supervisione strategica, che definisce e identifica il livello di rischio accettato (c.d. "appetito al rischio" e "tolleranza al rischio")", si ritiene utile stabilire in questa sede se, ove la lettura delle norme non consenta alla banca una univoca interpretazione delle stesse, possa essere adottato l'approccio di risk tollerance anche per il rischio di non conformità alle norme, ovvero se questo sia incluso nella definizione di rischio operativo.

❖ <u>Sezione II, par. 2 e 3; Sezione III, par. 3.3 - Identificazione delle operazioni di maggior rilievo oggetto del parere preventivo della funzione di controllo dei rischi</u>

<u>BOX 2</u>

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

Una operazione di maggior rilievo è solitamente una transazione non ricorrente, inabituale, significativa per dimensione e generalmente complessa: scadenza insolitamente lontana, dimensione eccezionale, complessa in termini di remunerazione, del sistema delle garanzie e più generalmente della strutturazione dell'operazione (algoritmi o strutture di pricing complessi o caratteristiche che sollevino nuovi problemi legali, di compliance o regolamentari).

Rientrano tra quelle di maggior rilievo le operazioni che:

- comportano deroghe per tipologia di clientela o forme particolari di garanzie;
- hanno ad oggetto un prodotto o servizio non disciplinato dalle procedure interne della Banca;
- in considerazione delle caratteristiche tipiche della controparte, comportano l'esposizione della Banca ad un rischio rilevante;
- risultano atipiche dal punto di vista della sostanza e della finalità economica, quali ad esempio trasferimenti circolari dei rischi, operazioni con orizzonti inabitualmente brevi;
- le cui condizioni economiche significative non sono conformi alle norme o alle pratiche di mercato;
- hanno un carattere inabituale o particolarmente complesso rispetto all'attività economica del cliente;
- presentano una struttura giuridica inabituale o particolarmente complessa;

- risultano potenzialmente rilevanti ai fini regolamentari o in materia di rischi reputazionali sia per il Gruppo, sia per a singola entità operativa;
- complesse ai fini della "trasparenza";
- danno luogo ad un profitto, una perdita inabituale o a una remunerazione che sembra nettamente sproporzionata rispetto ai servizi prestati, all'investimento effettuato o al rischio di credito, rischio di mercato o rischio operativo assunto dall'entità;
- non possono essere trattate attraverso i sistemi riconosciuti o che pongono delle rilevanti difficoltà di trattamento da parte del middle e back-office.

❖ Sezione II, par. 5 - Il coordinamento delle funzioni di controllo

[...] *Per assicurare una corretta interazione tra tutte le funzioni e organi con compiti di controllo, evitando sovrapposizioni o 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/organi e tra queste/i e gli organi aziendali e, nel caso in cui gli ambiti di controllo presentino aree di potenziale sovrapposizione o permettano di sviluppare sinergie, le modalità di coordinamento e di collaborazione. A titolo esemplificativo, nell'attività dell'organismo di vigilanza, che attiene in generale all'adempimento di leggi e regolamenti, può essere proficuo uno stretto raccordo, in termini sia di suddivisione di attività che di condivisione di informazioni, con le funzioni di conformità alle norme e di revisione interna.[...]*

Giacché la previsione richiede di descrivere lo specifico impianto organizzativo adottato da una Banca/un Gruppo per la delineazione delle proprie funzioni di controllo interno, appare la sede propria anche per dare evidenza di eventuali tipicità eventualmente tratte da Capogruppo estere. Si propone dunque di integrare la previsione contemplando la fattispecie come segue:

- "*Per assicurare una corretta interazione tra tutte le funzioni e organi con compiti di controllo, evitando sovrapposizioni o lacune, anche a fronte di eventuali indirizzi di Gruppo rispondenti a diversi ordinamenti, l'organo con funzione di supervisione strategica ...*".

❖ Sezione III, par. 1- Declinazione del principio di proporzionalità

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 tal 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*

Si chiede di valutare se, avuto riguardo all'esigenza di assicurare un rapporto ottimale costi/benefici nell'articolazione e nella conduzione dei controlli, la declinazione del principio di proporzionalità possa prevedere anche la possibilità di non istituire la funzione di revisione interna laddove l'organizzazione dei controlli di 1° e 2° livello e le caratteristiche dell'attività lo consentano (previsione già contemplata nel Regolamento congiunto Banca d'Italia e Consob in materia di servizi di investimento), per quelle entità che, facendo parte di un Gruppo Bancario, sono comunque soggette/ assoggettabili a controlli di revisione interna da parte della Capogruppo sulla base di un sistema di controllo di terzo livello integrato e omogeneo per l'intero Gruppo.

In particolare, si chiede di valutare se, una tale previsione possa essere integrata nell'ambito della Sezione V, "Il sistema dei controlli interni nei Gruppi Bancari" individuando per le controllate vigilate di un Gruppo bancario la facoltà di non istituire la funzione di revisione interna laddove l'organizzazione dei controlli di 1° e 2° livello e le caratteristiche dell'attività della controllata nonché l'organizzazione della revisione interna della Capogruppo lo consentano. Ciò comporterebbe infatti il beneficio di un'organizzazione della revisione interna integrata nel Gruppo Bancario, la quale utilizzerebbe risorse proprie direttamente presso l'entità sulla base del piano di audit risk based (eliminando peraltro gli oneri connessi alla nomina di un referente per l'internal audit interno all'entità del Gruppo). In tal caso verrebbe meno l'applicazione di ogni previsione relativa all'esternalizzazione della funzione di revisione interna per le entità dello stesso Gruppo Bancario.

Con riferimento alla declinazione nel concreto del principio, tra i criteri per determinare la complessità dimensionale si possono annoverare, ad esempio, il fatturato, il numero dei dipendenti, il numero dei canali di vendita, il numero di dipendenze.
La complessità operativa, a sua volta, è legata al tipo di servizio/prodotto reso (multi prodotto-mono prodotto); ulteriore indice di complessità può essere rappresentato dalla notevole dotazione di risorse umane e tecnologiche per l'ingresso in un determinato business, tale da costituire una barriera all'ingresso per altri concorrenti, operatività transfrontaliera.

Infine, per le banche con approccio di vigilanza home – host è importante prevedere la possibilità di mantenere un approccio flessibile sull'assetto organizzativo delle funzioni di controllo, in coerenza con quello delle banche estere capogruppo, atto a garantire a livello di gruppi internazionali l'omogeneità delle soluzioni organizzative in tema di controlli interni.

❖ Sezione III, par. 1 - Istituzione delle funzioni aziendali di controllo

Ferma restando l'autonoma responsabilità aziendale per le scelte effettuate in materia di assetto dei controlli interni, le banche istituiscono, secondo quanto di seguito indicato, funzioni aziendali di controllo permanenti ed indipendenti. [...]
[...] Per ***assicurare l'indipendenza delle funzioni aziendali*** *di controllo è necessario che: [...]*
b) i responsabili possiedono ***requisiti di professionalità*** *e siano collocati in posizione gerarchico – funzionale adeguata. [...] 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 [...]*
d) le funzioni aziendali di controllo siano tra loro separate, sotto un profilo organizzativo. [...]
e) i criteri di remunerazione del personale che partecipa alle funzioni aziendali di controllo non ne compromettano l'obiettività e concorrano a creare un sistema di incentivi coerente con le finalità della funzione svolta [...]
[...] Se coerente con il principio di proporzionalità, le banche possono, a condizione che i controlli sulle diverse tipologie di rischio continuino ad essere efficaci: [...] affidare lo svolgimento delle funzioni aziendali di controllo all'esterno [...]

In relazione alla previsione dei **requisiti di professionalità**, sarebbe opportuno esplicitare in questa sede quali sono tali requisiti.

Con riferimento ai **criteri di remunerazione**, in considerazione della dichiarata esigenza di offrire un quadro disciplinare organico della diversa regolamentazione intervenuta negli anni sulla materia e, tra queste, la disciplina delle Politiche di Remunerazione, si ravvisa l'opportunità di richiamare in quest'ambito anche le responsabilità in materia di determinazione della remunerazione dei responsabili delle funzioni di controllo.

Tenuto conto che in taluni contesti, a fronte dell'esigenza di costituire presidi a salvaguardia dell'indipendenza delle funzioni di controllo che appare sottesa alla previsione, si prevedono anche raccordi con le omologhe funzioni di Capogruppo, si propone di integrare la previsione stessa come segue:

- *"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 nonché eventuali omologhe funzioni di Gruppo".*

Infine per quanto riguarda la prevista facoltà di accorpare/esternalizzare le funzioni di controllo in base al principio di proporzionalità, si rimanda alle osservazioni formulate al punto 3 del presente documento *(BOX 3 - Declinazione del principio di proporzionalità (Capitolo 7, Sezione II, par. 1)).*

❖ Sezione III par. 3 - Requisiti specifici delle funzioni aziendali di controllo

Particolare attenzione deve essere posta anche nella ***verifica della conformità dell'attività aziendale alle normative di natura fiscale****, al fine di evitare di incorrere in violazioni o elusioni di tale normativa ovvero in situazioni di abuso del diritto, che possono determinare [...]*
[...] La funzione di controllo dei rischi (Risk Management) ha la finalità di attuare le politiche di governo dei rischi...il responsabile della funzione può essere collocato alle dirette dipendenze del comitato controllo e rischi o dell'organo con funzione di supervisione strategica (per le banche SREP 1 e 2 è obbligatorio).

[...] La funzione di revisione interna [...] sulla base dei risultati dei propri controlli formula ***raccomandazioni agli organi aziendali*** *[...] coerentemente con il piano di audit [...]*
- valuta la conformità dell'operatività aziendale al livello di tolleranza al rischio/ appetito per il rischio approvato dall'organo con funzione di supervisione strategica e, in caso ***di strutture finanziarie particolarmente complesse****, la conformità di queste alle strategie approvate dagli organi aziendali;*
- verifica, anche attraverso accertamenti di natura ispettiva a) la regolarità delle diverse attività aziendali, incluse quelle esternalizzate, e l'evoluzione dei rischi sia nella direzione generale della banca, sia nelle filiali. La ***frequenza delle ispezioni deve essere coerente con l'attività svolta****.[...] g) la rimozione delle anomalie riscontrate nell'operatività e nel funzionamento dei controlli (attività di "follow-up") [...]*
- ***espleta compiti d'accertamento anche con riguardo a specifiche irregolarità****, ove richiesto dagli organi aziendali;*
- ***controlla regolarmente il piano aziendale di continuità operativa.*** *In tale ambito, prende visione dei programmi di verifica, assiste alle prove e ne controlla i risultati, propone modifiche al piano sulla base delle mancanze riscontrate. La funzione di revisione interna è coinvolta nel controllo dei piani di emergenza degli outsourcer e dei fornitori critici; essa può decidere di fare affidamento sulle strutture di questi ultimi, se ritenute professionali ed indipendenti quanto ai risultati dei controlli ed esamina i contratti per accertare che il livello di tutela sia adeguato agli obiettivi e agli standard aziendali;*
- nell'ambito della ***collaborazione e dello scambio di informazioni con il soggetto incaricato della revisione legale dei conti, individua le criticità emerse durante l'attività di revisione*** *e si attiva affinché le competenti funzioni aziendali adottino i presidi necessari per superare tali criticità. [...]*
Con specifico riferimento al processo di gestione dei rischi *[...] valuta: [...]*
- l'appropriatezza delle ipotesi utilizzate nelle analisi di scenario e negli stress test;
- l'allineamento con le best pratiche diffuse nel settore
[...] Fermo restando che la funzione non va posta sotto la dipendenza gerarchica di responsabili di aree operative, ***il grado di autonomia può essere accresciuto con la collocazione alle dirette dipendenze del comitato controllo e rischi, ove costituito, o dell'organo con funzione di supervisione strategica****. Ciò non preclude, tuttavia, la contestuale esigenza di salvaguardare i raccordi con l'organo con funzione di gestione, che deve poter esercitare le proprie prerogative ai fini di concorrere all'indirizzo* ***delle attività di revisione interna****. [...]*

Nel definire i requisiti specifici delle funzioni aziendali di controllo il presente documento pare voler attribuire alla "Compliance" la funzione di verifica della conformità dell'attività aziendale alla normativa fiscale.

Non si ritiene tale scelta efficiente, per i seguenti principali motivi:

- Tale scelta appare inefficiente e costosa: l'attribuzione di tale compito alla Direzione Compliance richiederebbe infatti la necessità di prevedere l'allocazione di personale specializzato nell'ambito tributario anche all'interno della predetta Direzione. Ciò comporterebbe una indubbia duplicazione di competenze tecniche (dislocate prevalentemente della Funzione fiscale e parzialmente nella funzione Compliance) e conseguentemente di costi, attesa la necessità di formazione e aggiornamento costante, che la specifica materia richiede. Formazione e aggiornamento spesso possibile, peraltro, solo attraverso l'analisi e l'approfondimento di specifiche operazioni o attività, già compito della Funzione fiscale, con la quale dunque occorrerebbe prevedere anche forme di coordinamento e di scambio di informazioni, con conseguenti inefficienze in termini di svolgimento dell'attività lavorativa.
- Tale scelta appare incoerente con l'indicazione che sembra al contrario emergere dalle disposizioni attualmente in discussione da parte del legislatore fiscale. La cosiddetta Delega Fiscale, attualmente in discussione (AC 5291), introduce una previsione espressa in tema di sistemi di gestione e controllo del rischio fiscale da parte delle aziende di maggiori dimensioni, la cui istituzione (opzionale) all'interno delle predette aziende sarà assistita da un sistema premiale in tema di minori adempimenti e sanzioni. Dalla Relazione al Disegno di legge emerge una attribuzione di tale compito e delle relative responsabilità alle Funzioni fiscali.

L'attribuzione alla Funzione fiscale risulta certamente più adeguata e razionale, soprattutto nei casi in cui a tale Funzione non competa lo svolgimento degli adempimenti oggetto di controllo (situazione quest'ultima che richiederebbe una necessaria rideterminazione delle relative *mission*).

La gestione del rischio sarebbe attuata con l'istituzione, ove già non esistenti, o l'eventuale implementazione, di appositi processi, periodicamente revisionati e ampliati numericamente in dipendenza dello svilupparsi di nuove aree di rischio, queste ultime individuate dalla Funzione fiscale, a seguito dei controlli e dell'attività di consulenza dalla stessa svolta ovvero per effetto di modifiche normative. Tali processi prevederebbero, per quanto possibile, che nelle specifiche aree individuate sia richiesto il preventivo benestare della Funzione fiscale per la conclusione delle operazioni/attività/adempimenti. In assenza di tale benestare, l'organo di gestione o di supervisione strategica potrà ugualmente disporre di procedere, assumendosi il relativo rischio.
Tali processi, attualmente operanti per l'approvazione dei nuovi prodotti e, nell'ambito della imposizione societaria, con riferimento a talune aree di rischio, sarebbero invece estesi anche ad altri settori.

La Compliance avrà il compito esclusivo di coordinare e monitorare i sistemi di controllo del rischio, anche attraverso organi inseriti nell'ambito della medesima Direzione di appartenenza della Funzione fiscale.

Quindi si propone di integrare la frase

- *"Particolare attenzione deve essere posta anche nella* ***verifica della conformità dell'attività aziendale alle normative di natura fiscale****, al fine di evitare di incorrere in violazioni o elusioni di tale normativa ovvero in situazioni di abuso del diritto, che possono determinare [...]"*

con

- *"Lasciare all'autonomia organizzativa degli intermediari il conferimento di attribuzioni e connessi doveri inerenti alla* ***gestione del rischio di non conformità dell'attività aziendale alle normative di natura fiscale.***

Inoltre, con riferimento alla previsione

- *"In relazione ai molteplici profili professionali richiesti per l'espletamento di tali adempimenti, le varie fasi in cui si articola l'attività della funzione di conformità alle norme possono essere affidate a strutture organizzative (es. legale, organizzazione, gestione del rischio operativo), purché il processo di gestione del rischio e l'operatività della funzione siano ricondotti ad unità mediante la nomina di un responsabile che coordini e sovrintenda alle diverse attività"*

considerata la pervasività della normativa nel campo bancario e finanziario, sarebbe opportuno in questa sede esplicitare ancora più chiaramente con quali modalità il responsabile dovrebbe "*coordinare e sovrintendere le diverse attività*" svolte da ruoli che trattano materie di compliance inseriti in altre strutture, ad esempio ruoli spesso deputati a tradurre in requisiti funzionali o presidi organizzativi i mutevoli adattamenti normativi.

Con specifico riferimento alla funzione di Risk Management il suo collocamento esclusivamente alle dirette dipendenze degli organi di governo collegiali comportebbe uno "scollamento" rispetto alle attività gestionali riducendone l'ambito ad una attività di "mero monitoraggio" che rappresenterebbe un "ritorno al passato" rispetto all'evoluzione del Risk Management osservate nei recenti esercizi.

D'altronde è la stessa normativa che richiede al contempo una non eccessiva distanza del Risk Management dal business (come garanzia di una maggiore consapevolezza dei rischi) e che esprima pareri preventivi per le operazioni di maggior rilievo.

Si propone quindi di attenuare questo concetto prevedendo al un riporto congiunto all'Amministratore delegato e agli organi collegiali.

Con specifico riferimento alla previsione relativa alla revisione interna:

- "*sulla base dei risultati dei propri controlli formula* ***raccomandazioni agli organi aziendali***"

considerando che per **organi aziendali** si intende (vedi definizione pag. 3 del documento di consultazione) "*il complesso degli organi con funzioni di supervisione strategica, di gestione e di controllo*", si chiede se si vuole che la funzione di revisione interna emetta raccomandazioni, ad esempio, destinate al Consiglio di Amministrazione che è l'organo che nomina e revoca i responsabili delle funzioni di controllo oppure raccomandazioni verso il Collegio Sindacale che è invece l'organo che ha la responsabilità di vigilare sulla completezza, funzionalità e adeguatezza del sistema dei controlli interni, di cui anche la revisione interna è parte integrante.

Con specifico riferimento alla previsione secondo cui la revisione interna:

- valuta la conformità di ***strutture finanziarie particolarmente complesse*** alle strategie approvate dagli organi aziendali,

si chiede una qualificazione, esemplificazione della fattispecie.

Con specifico riferimento alla previsione relativa alla revisione interna:

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

avuto riguardo all'esigenza di assicurare un rapporto ottimale costi/benefici nell'articolazione e nella conduzione dei controlli[3], si chiede di valutare se la frequenza delle ispezioni possa essere coerente anche con il grado di penetrazione e diffusione dei controlli di 1° e 2° livello sia nella direzione generale della banca, sia nelle filiali.

Segnatamente si chiede di valutare se ove siano già previsti nel piano dei controlli di 1° e 2° livello, accertamenti di natura ispettiva sulla regolarità delle diverse attività aziendali in ciascuna filiale da effettuare in un dato arco temporale, alla Funzione di Revisione Interna sia consentito di procedere per eccezioni e dunque operare la revisione interna delle Direzioni territoriali contemplando interventi nelle collegate strutture periferiche/filiali su base campionaria.

Dunque si propone la seguente modifica:

- *La frequenza e la diffusione delle ispezioni deve essere coerente sia con l'attività svolta, sia con la frequenza e la diffusione delle verifiche già assicurate dai controlli di 1° e 2° livello.*

Tenuto altresì conto di quanto al riguardo ad oggi previsto dalla Banca d'Italia nel Provvedimento recante disposizioni attuative in materia di organizzazione, procedure e controlli interni in materia di antiriciclaggio, in cui si stabilisce che per la revisione interna "gli interventi, sia a distanza che ispettivi, devono essere oggetto di pianificazione per consentire che **tutte le strutture operative periferiche e centrali** siano sottoposte a verifica in un **congruo arco di tempo** e che le iniziative siano più frequenti nei confronti delle strutture maggiormente esposte ai rischi di riciclaggio e di finanziamento del terrorismo", si chiede di valutare una previsione di coordinamento tra la disciplina in esame e detto Provvedimento che in ultimo consenta alla revisione interna di programmare i propri interventi sulle strutture centrali e periferiche con una frequenza e con tecniche di campionamento univoci (sia che siano guidate dal rischio antiriciclaggio, sia da altri rischi).

Si rileva inoltre il mancato riferimento alla **funzione antiriciclaggio** e, conseguentemente, il **mancato coordinamento** con il provvedimento Organizzativo della Banca d'Italia del 10 marzo 2011.
Il presente documento in consultazione - che si propone quale obiettivo quello di disegnare la materia dei *sistemi dei controlli interni* - tratta della funzione di compliance e relativamente ad essa sancisce l'esplicita abrogazione del relativo provvedimento ("Disposizioni di vigilanza - la funzione di controllo di conformità alle norme delle banche"), ma nulla prevede con riferimento alla funzione antiriciclaggio.
Alla luce di quanto stabilito dal provvedimento di Banca d'Italia che espressamente prevede che "*L'impresa si dota di una funzione specificatamente deputata a prevenire e contrastare la realizzazione di operazioni di riciclaggio e di finanziamento del terrorismo*" e che "*il responsabile antiriciclaggio rientra, a tutti gli effetti, nel novero dei responsabili di funzioni aziendali di controllo*", si richiede pertanto di integrare il documento in parola, quantomeno con una disciplina che tenga in considerazione il coordinamento con il provvedimento antiriciclaggio.

Con specifico riferimento alla previsione relativa alla revisione interna:

- ***"compiti d'accertamento anche con riguardo a specifiche irregolarità"***[4]

---

[3] Declinazione del principio di proporzionalità - Capitolo 7, Sezione III – par. 1. Istituzione delle funzioni aziendali di controllo.
[4] Nella Sezione I – par. 6. Principi Generali tra le tipologie di controllo è previsto " [...] revisione interna (c.d. "controlli di terzo livello"), volta ad individuare andamenti anomali, **violazione delle procedure e della regolamentazione** [...]".

per escludere che vi si legga una sorta di riserva di attività in capo alla revisione interna, come già sopra osservato (Commenti su "Principi generali"), si propone di valutare se espressamente diffondere in capo ai diversi livelli di funzione di controllo tale obbligo.

Anche in ordine alla rilevanza della cultura del controllo statuita alla Sezione I. Paragrafo 6. Principi Generali, si propone dunque di:

- eliminare le specifiche previsioni nei brani puntualmente riferiti alla revisione interna e di integrare come segue la Sezione I. Paragrafo 6. Principi Generali, Pagine 5 3°cpv.:

  "Per poter realizzare questo obiettivo, il sistema dei controlli interni deve in generale: (...)individuare violazioni delle procedure e della regolamentazione ed accertare specifiche irregolarità";

- integrare come segue la Sezione I. Paragrafo 6. Principi Generali, Pagine 5 3°cpv.:

  "Per poter realizzare questo obiettivo, il sistema dei controlli interni deve in generale: accertare specifiche irregolarità (...) ".

Con specifico riferimento alla previsione relativa alla revisione interna:

- ***controllare regolarmente il piano aziendale di continuità operativa,***

si chiede – in generale – se tale previsione possa essere riformulata diffondendo il presidio del piano aziendale di continuità operativa che fu delineato nel 2004 in modo maggiormente aderente all'attuale articolazione delle funzioni di controllo successivamente sviluppata. In particolare si propone di valutare di lasciare in capo alla revisione interna l'obbligo di un verifica (per esempio, definendolo "almeno annuale", in analogia a quanto previsto per altre tematiche rilevanti) che abbia ad oggetto i temi succitati, ma di attribuire l'obbligo di assistere alle relative prove e di controllarne i risultati a strutture più propriamente interessate a verifiche di prossimità e di natura permanente.

Dunque si propone di modificare la previsione come segue:

- *"La funzione di revisione interna controlla periodicamente (ovvero almeno annualmente) il piano aziendale di continuità operativa. In tale ambito, esamina i programmi di verifica, i risultati delle prove, i piani di emergenza degli outsourcer e dei fornitori critici ovvero esamina i relativi contratti per accertare che il livello di tutela sia adeguato agli obiettivi e agli standard aziendali".*

Si propone altresì di specificare in altra parte della disciplina l'obbligo di effettuare regolarmente verifiche di conformità del piano aziendale di continuità operativa e delle relative prove.

In tema di

- **collaborazione e scambio di informazioni con il soggetto incaricato della revisione legale dei conti,**

tenuto conto che le criticità emerse durante l'attività di revisione del soggetto stesso vengono anche attestate in modo formale e che i flussi informativi e le relazioni con detto soggetto sono variamente articolate nelle diverse organizzazioni, si chiede di valutare se la modalità operativa da esperire affinché le competenti funzioni aziendali adottino i presidi necessari per superare tali criticità, non possa essere assegnata in generale alla Banca (che la declinerà in base al proprio modello di funzionamento) piuttosto che alla revisione interna.

Dunque si propone di togliere la linea dalla descrizione delle attribuzioni della revisione interna e di riformularlo in capo alla Banca in altra parte della disciplina.

Infine, in analogia a quanto già osservato con riferimento a **nomina e revoca dei responsabili delle funzioni di controllo**[5], tenuto conto che in taluni contesti, a fronte dell'esigenza di costituire presidi a salvaguardia dell'indipendenza della funzione di revisione interna, si prevedono anche raccordi con le omologhe funzioni di Capogruppo, si propone di integrare la previsione posta al par. 3.4. come segue:

- *"Fermo restando che la funzione non va posta sotto la dipendenza gerarchica di responsabili di aree operative, il grado di autonomia può essere accresciuto con la collocazione alle dirette dipendenze del comitato controllo e rischi, ove costituito, o dell'organo con funzione di supervisione strategica o ad omologhe funzioni di Gruppo. Ciò non preclude, tuttavia, la contestuale esigenza di salvaguardare i raccordi con l'organo con funzione di gestione, che deve poter esercitare le proprie prerogative ai fini di concorrere all'indirizzo delle attività di revisione interna".*

❖ Sezione V - Il Sistema dei Controlli Interni nei Gruppi Bancari

La capogruppo, nel quadro dell'attività di direzione e coordinamento del gruppo, deve esercitare:

a) *un controllo strategico sull'evoluzione delle diverse aree di attività in cui il gruppo opera e dei rischi incombenti sulle attività esercitate. Si tratta di un controllo sia sull'andamento delle attività svolte dalle società appartenenti al gruppo (crescita o riduzione per via endogene), sia sulle politiche di acquisizione e dismissione da parte delle società del gruppo (crescita o riduzione per via esogena);*
b) *un controllo gestionale volto ad assicurare il mantenimento delle condizioni di equilibrio economico, finanziario e patrimoniale sia delle singole società, sia del gruppo nel suo insieme. Queste esigenze di controllo vanno soddisfatte preferibilmente attraverso la predisposizione di piani, programmi e budget (aziendali e di gruppo), e mediante l'analisi delle situazioni periodiche, dei conti infra-annuali, dei bilanci di esercizio delle singole società e di quelli consolidati; ciò sia per settori omogenei di attività sia con riferimento all'intero gruppo;*
c) *un controllo tecnico-operativo finalizzato alla valutazione dei vari profili di rischio apportati al gruppo dalle singole controllate e dei rischi complessivi del gruppo.*

Le capogruppo che esercitano l'attività di direzione e coordinamento in violazione dei principi di corretta gestione societaria e imprenditoriale sono responsabili ai sensi degli artt. 2497 e ss del codice civile.

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

- *all'interno di tutte le banche del gruppo e delle altre entità che, a giudizio della capogruppo, assumono rischi considerati rilevanti per il gruppo nel suo complesso vengono individuati appositi referenti i quali: svolgono **compiti di supporto** per la funzione aziendale di controllo esternalizzata; **riportano funzionalmente e gerarchicamente** a quest'ultima; provvedono tempestivamente a segnalare eventi o situazioni particolari, suscettibili di modificare i rischi generati dalla controllata*
- *qualora l'esternalizzazione sia effettuata alla capogruppo, all'interno della funzione di revisione interna della stessa viene mantenuta un'adeguata separazione tra le unità e le risorse deputate a svolgere l'internal audit su base individuale per le controllate da quelle responsabili dei controlli su base consolidata le quali, tra i diversi compiti, hanno anche quello di verificare la funzionalità del complessivo sistema dei controlli interni di gruppo.[...]*

[5] Sezione III – par. 1. Istituzione delle funzioni aziendali di controllo.

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

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

La previsione di un riporto funzionale e gerarchico del referente della funzione di revisione interna esternalizzata alla stessa funzione può confliggere con l'attribuzione di ulteriori ruoli e responsabilità a detto referente in seno all'entità interessata e quindi con l'indipendenza e obiettività della funzione di revisione interna rispetto alle ulteriori attività svolte da detto referente. Tale previsione appare peraltro anche difficilmente coordinabile con quella indicata nella sez. IV (esternalizzazione di funzioni aziendali (outsourcing), paragrafo 1 "principi generali e requisiti particolari"[6] che obbliga la funzione di revisione interna a dare riscontro tempestivamente a qualsiasi richiesta di informazioni e consulenza da parte del referente per l'attività esternalizzata (oltre che degli organi aziendali).

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

Si chiede di valutare se al fine di segregare le competenze della Capo Gruppo rispetto a quelle delle controllate, possa essere sufficiente definire ex ante, per esempio in sede di approvazione dei Piani di Audit, gli equivalenti in termini di effettivi (c.d. FTE) assegnati su base individuale alle controllate. Tale previsione consentirebbe peraltro una maggiore flessibilità nell'adottare modelli organizzativi convergenti con le indicazioni di cui alla sez. III par 1 "istituzione delle funzioni aziendali di controllo" in cui si dice che "*la banca incentiva, all'interno delle singole funzioni di controllo, programmi di rotazione delle risorse*".

Si propone dunque di modificare la previsione come segue

- "*qualora l'esternalizzazione sia effettuata alla capogruppo, all'interno della funzione di revisione interna della stessa viene identificata un'adeguata e preventiva quantificazione degli effettivi deputati a svolgere il piano di internal audit su base individuale per le controllate da quelli deputati a svolgere quello su base consolidata che, tra i diversi compiti, hanno anche quello di verificare la funzionalità del complessivo sistema dei controlli interni di gruppo*".

---

[6] "Le banche di dimensioni contenute o caratterizzate da una limitata complessità operativa che intendono affidare a soggetti terzi, in tutto o in parte, le funzioni aziendali di controllo definiscono nell'accordo di esternalizzazione, le modalità e la frequenza della reportistica dovuta al referente per l'attività esternalizzata e agli organi aziendali sulle verifiche effettuate. Resta fermo l'obbligo di dare riscontro tempestivamente a qualsiasi richiesta di informazioni e consulenza da parte di questi ultimi che in ogni caso rimangono responsabili del corretto espletamento delle attività di controllo esternalizzate".

❖ Sezione VII - Procedure di Allerta Interna

[...]con riferimento ai soggetti che possono ricevere le segnalazioni[7], le procedure prevedono diverse opzioni a disposizione del segnalante in modo da consentire che il soggetto che riceve la segnalazione non sia gerarchicamente subordinato all'eventuale soggetto segnalato (ad es. il soggetto segnalante deve essere in grado di segnalare la criticità al suo responsabile operativo, al responsabile della funzione di revisione interna, al presidente del comitato controllo e rischi, al presidente dell'organo di controllo).[...]

Con riferimento ai soggetti che possono ricevere le segnalazioni di allerta interno, le nuove istruzioni stabiliscono che può essere destinatario delle stesse il responsabile della funzione di revisione interna e non c'è alcun riferimento espresso al Funzione di conformità. Si suggerisce di annoverare tra i soggetti destinatari di tali segnalazioni anche la Funzione Compliance.

TITOLO V – CAPITOLO VIII - Sistema Informativo

❖ Sezione II, par. 1 - Interazioni tra rischio informatico e rischi operativi

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.***

Il rischio informatico (di seguito rischio IT) è considerato alla stregua degli altri rischi operativi e pertanto è sottoposto ai medesimi processi di mappatura nella cartografia dei rischi della BNL e di valutazione dei medesimi. Tale rischio può derivare da eventi di diversa natura che generano un'interruzione, una discontinuità operativa o un'azione fraudolenta correlata all'attività informatica che determinano perdite o costi addizionali per la Banca.

L'impatto sul rischio operativo di questa tipologia di incidenti deriva sia dagli effetti economici sia dagli effetti sul business (perdita di redditività e mancato guadagno) nonchè sulla reputazione aziendale.

Al fine di valutare il rischio operativo di natura informatica sono utilizzati i seguenti elementi:

a. *Costi di ripristino*:
   - Sistemazione dei programmi degradati
   - Sostituzione degli asset danneggiati
   - Recupero dei dati
   - Costi di lavorazione straordinari
   - Costi relativi a comitati di crisi
   - Costi derivanti da extra budget o abbandono di progetto informatico

b. *Altre componenti di costo*:
   - Perdita di redditività/mancato guadagno
   - Interessi di mora
   - Sanzioni

[7] Cfr. sez III par.1 (iii di revisione interna)

- Spese legali
- Degrado del livello reputazionale
- Perdita per frode informatica

Per la valorizzazione di alcune tra queste tipologie di incidenti e l' individuazione delle azioni di mitigazione dei relativi rischi si fa riferimento anche al Business Continuity Plan ed al Piano di Disaster Recovery integrate nel più ampio ambito dell'Information Security Management System (ISMS).

❖ Sezione III, punti A ed E - La Gestione del rischio informatico

"[...] il rischio residuo deve essere trattato con presidi compensativi, ad esempio di tipo organizzativo o procedurale, anch'essi documentati e sottoposti all'accettazione formale dell'utente responsabile. [...]"

Per rendere più chiaro il fatto che le misure a contenimento del rischio residuo possono essere previste solo nel caso in cui la banca decida di inserire nuovi presidi per contenere il rischio residuo medesimo, formuliamo la seguente proposta di revisione:

"Per i sistemi già in esercizio, gli eventuali presidi ***che la banca decida di aggiungere rispetto*** *a quelli già operativi, formano l'oggetto di uno specifico piano di implementazione, con l'indicazione dei tempi di realizzazione. Nelle more dell'attuazione del piano, il rischio residuo* ***può*** *essere trattato con presidi compensativi, ad esempio di tipo organizzativo o procedurale, anch'essi documentati e sottoposti all'accettazione formale dell'utente* ***dell'applicazione."***