Position Paper
Gruppo Bancario Iccrea

In risposta alla consultazione della Banca d'Italia "Sistema dei controlli interni, sistema informativo e continuità operativa"

Sommario

Procedura Consultazione Banca d'Italia: Disposizioni in materia di Controlli Interni, Sistema Informativo e Continuità Operativa

Per integrazione ed ulteriore supporto – per taluni aspetti – a quanto trasmesso dall'Associazione di Categoria, nel seguito si riportano le considerazioni che Iccrea Holding S.p.a., in qualità di Capogruppo del Gruppo Bancario Iccrea, sottopone al vaglio di codesto Spettabile Organo di Vigilanza relativamente alle Disposizioni in consultazione.

Capitolo 7 – Il Sistema dei Controlli Interni

3. Definizioni

Pag.3: << *e) -"Funzioni aziendali di controllo": la funzione di conformità alle norme (compliance), la funzione di controllo dei rischi (risk management function) e la funzione di revisione interna (internal audit).*>>

In relazione alle diverse possibili scelte aziendali nell'articolazione delle funzioni controllo, si propone la seguente formulazione: Funzioni aziendali di controllo": la funzione di conformità alle norme (compliance), la funzione antiriciclaggio, ove non ricompresa in altre funzioni, la funzione di controllo dei rischi (risk management function) e la funzione di revisione interna (internal audit).

Sezione II – Il ruolo degli organi aziendali

Diversamente dall'attuale contesto normativo (cfr. Circolare 239 TIT .IV Cap.11 Sez. II Par.-Ruolo del Consiglio di Amministrazione e dell'Alta direzione) le disposizioni in consultazione non regolamentano in modo esplicito ruolo, compiti e responsabilità del Direttore Generale nell'ambito del sistema dei controlli interni. In effetti, la nuova normativa, relativamente a detto esponente aziendale prevede esclusivamente che "il direttore generale rappresenta il vertice della struttura interna e come tale partecipa alla funzione di gestione".

Pur avendo presente che le nuove disposizioni prendono atto dell'evoluzione nell'ambito del sistema bancario dell'assetto degli Organi aziendali (da assetto tradizionale a sistema monistico o dualistico) non sembra ultroneo prevedere un riferimento esplicito, per quanto in forma sintetica, a ruolo, compiti e responsabilità del direttore generale nel sistema dei controlli interni, specie laddove l'assetto organizzativo si riferisca ancora al modello tradizionale.

L'intervento implementativo proposto potrebbe, ad esempio, consistere nell'introduzione di una prescrizione minimale del seguente tenore: "Il direttore generale, specie nel modello tradizionale, può essere destinatario di deleghe da parte dell'Organo con funzione di supervisione strategica in materia di strutturazione e funzionamento del sistema dei controlli interni".

Si ritiene che una tale previsione consentirebbe anche di meglio definire le responsabilità del direttore generale eventualmente riconducibili nella sfera del procedimento sanzionatorio per violazioni delle prescrizioni normative applicabili alle Banche.

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

Si evidenzia inoltre che l'intero impianto normativo con riferimento al ruolo degli organi aziendali nel sistema dei controlli interni, appare precipuamente improntato a disciplinare i compiti di governo dei rischi in un assetto di organi proprio del sistema duale, fornendo "indicazioni minime circa il ruolo di ciascun organo aziendale nell'ambito del sistema dei controlli interni, anche al fine di chiarire i relativi compiti e responsabilità" pur non esaurendo dette indicazioni "le cautele che possono essere adottate dai competenti organi aziendali nell'ambito della loro autonomia gestionale" (punto 1. Premesse).

Nel contesto organizzativo proprio del Sistema duale appaiono molto ben definiti i compiti dell'Organo con Funzione di Supervisione Strategica (Consiglio di Sorveglianza ai sensi dell'art. 2409 duodecies e ss. Cod.Civ.) e quelli propri dell'Organo con Funzione di Gestione (Consiglio di Gestione ai sensi dell'art.2409 novies e ss. Cod.Civ.), rispondendo le previsioni di cui al punto 2) ed al punto 3) della Sez. II ad una ripartizione dei rispettivi ruoli di detti Organi nelle politiche di governo dei rischi propria delle previsioni di cui all'art. 2409 octies e ss Cod.Civ..

Nel sistema tradizionale il Consiglio di Amministrazione è usualmente attributario di gran parte dei compiti sia di gestione che di supervisione strategica ripartiti su due organi (Consiglio di Gestione e Consiglio di Sorveglianza) nel sistema duale. Ad una interpretazione analogica estensiva della normativa di cui punto 3) Sez. II del documento in consultazione, si potrebbe ipotizzare di incentrare i relativi compiti definiti per l'Organo con funzione di gestione sulla Direzione Generale con riferimento agli intermediari creditizi che adottino il sistema tradizionale.

Se questa è l'interpretazione applicativa che si intende dare alla normativa in esame, in assenza di norme specifiche del documento in consultazione, che disciplinino il ruolo degli Organi aziendali proprio del sistema tradizionale, si rappresenta che i compiti (ed i poteri) della Direzione Generale (non disciplinati dal Codice Civile) sono normalmente attribuiti da parte del Consiglio di Amministrazione con limiti ed ambiti di intervento definiti dallo Statuto sociale, in genere circoscritti alla gestione corrente ed alla esecuzione delle deliberazioni assunte dall'Organo amministrativo e, in alcuni casi, estesi alla facoltà di proposta. Nella comune esperienza, gli statuti sociali nel Sistema tradizionale, non attribuiscono alla Direzione Generale poteri propri ed autonomi rispetto al Consiglio di Amministrazione, né di gestione né di governo del rischio.

In tale contesto una assimilazione analogica dei compiti di governo del rischio stabiliti al punto 3) della Sez. II, propri dell'Organo con funzione di gestione a quelli della Direzione Generale di un intermediario creditizio che adotti il Sistema tradizionale, dovrebbe necessariamente comportare coerenti modifiche statutarie o, viceversa, avere una portata applicativa più circoscritta.

Ci si riferisce, in particolare, al compito di definire (e non proporre) il processo di gestione del rischio, stabilendo "limiti operativi all'assunzione delle varie tipologie di rischio, coerenti con il livello di rischio accettato (lett.a) punto 3)); al compito di stabilire le responsabilità delle strutture e delle funzioni aziendali coinvolte nel processo di gestione dei rischi, in modo che siano prevenuti potenziali conflitti di interesse

(lett. c) punto 3)); al compito di autorizzare le operazioni di maggiore rilievo oggetto di parere negativo da parte della funzione di controllo dei rischi e, se dal caso, autorizzarle, informando l'organo con funzione di supervisione strategica e l'organo con funzione di controllo (lett. d) punto 3)); al compito di definire i flussi informativi interni volti ad assicurare agli organi aziendali la piena conoscenza e governabilità di fattori di rischio (lett. e) punto 3)); al compito di definire il processo per approvare gli investimenti in nuovi prodotti o servizi (secondo alinea, punto3)); al compito di assicurare e attuare la politica aziendale in materia di esternalizzazione di funzioni aziendali (terzo alinea, punto 3)) ed, infine, a quello di assicurare quanto previsto dalle lett. a) e b), c) e d) del quarto alinea, punto 3).

Rispetto a tutte le sopra indicate tematiche e, più in generale, alle altre contemplate al punto 3) della Sez. II del documento, la Direzione Generale esercita poteri di proposta all'Organo amministrativo ed è responsabile dell'attuazione delle deliberazioni da questo assunte, ma, si sottolinea, non è normalmente attributaria di compiti propri, né per legge, né per disposizioni statutarie, come, invece, è il Consiglio di Gestione nel sistema dualistico.

Si ribadisce quindi l'esigenza di una più puntuale disciplina del ruolo degli Organi aziendali e, in particolare, della Direzione Generale, nei compiti di governo dei rischi per gli intermediari creditizi che adottano il sistema tradizionale ovvero una più esplicita previsione di adeguamento degli statuti sociali nell'ipotesi in cui le previsioni del punto 3) della Sez. II del documento in consultazione, si intendono esplicitamente riferirsi a compiti propri della Direzione Generale, per gli intermediari creditizi che adottano il Sistema tradizionale.

Sezione III – Funzioni Aziendali di Controllo

1. Istituzione delle funzioni aziendali di controllo

Pag. 16: <<*le funzioni aziendali di controllo siano tra loro separate, sotto un profilo organizzativo. I rispettivi ruoli e responsabilità devono essere formalizzati;*>>.

Pag. 16: <<*Se coerente con il principio di proporzionalità, le banche possono, a condizione che i controlli sulle diverse tipologie di rischio continuino ad essere efficaci: - affidare lo svolgimento della funzione di conformità alle norme alle strutture incaricate della funzione di controllo dei rischi;*>>.

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

Le funzioni RMF e FC appartengono entrambe all'area dei "controlli c.d. di secondo livello" e come anche evidenziato in diversi passaggi della Proposta di Disciplina, l'area dei Rischi Operativi della RMF e l'area di competenza della FC presentano "forti interrelazioni". Ferma restando la separatezza con la Revisione

Interna, inquadrata nell'area dei "controlli c.d. di terzo livello", è nostro parere che le interrelazioni suddette tra RMF, con particolare riferimento ai Rischi Operativi, e FC siano tali da non far escludere quale *first best* l'ipotesi di convergenza organizzativa, ossia di riconduzione organizzativa della RMF e della FC, pur distinte, nell'ambito di una complessiva area di controllo di secondo livello al cui vertice può figurare il Chief Risk Officer, CRO (in modo da assicurare la riconduzione a "corpo unico" di tutti i rischi aziendali in una figura in grado di poter esprimere agli Organi Aziendali una visione "olistica"). Le due funzioni peraltro operano:

- secondo analoghe caratteristiche del framework metodologico di identificazione, valutazione, monitoraggio e controllo;
- in continuità di profilo di rischio presidiato (il rischio di conformità promana di fatto dai rischi operativi);
- con riferimenti operativi e di governance aziendali analoghi nella dialettica volta ad un innalzamento dei livelli di presidio (mitigazione): organizzazione e processi, risorse umane, IT.

Quanto precede, si ritiene, indipendentemente dalla dimensione o dalla complessità operativa dell'intermediario.

Si richiede pertanto di riconsiderare il vincolo dell'applicabilità del principio di proporzionalità (la cui definizione puntuale potrebbe conseguentemente non renderlo applicabile ad intermediari di dimensione e complessità operativa sopra la soglia definita) nella scelta organizzativa relativa alle funzioni di "controllo c.d. di secondo livello" consentendo in via diretta e non subordinata alla proporzionalità che RMF e FC riportino al CRO (che ne costituisce sintesi e riferimento indipendente all'interno della Banca per gli Organi Aziendali).

Ove le suddette considerazioni non siano accolte si richiede che siano quantomeno specificati i *driver* alla base della valutazione di *first best* prudenziale dell'ipotesi di separatezza organizzativa tra le due funzioni al fine di poter valutare puntualmente gli elementi di attenuazione del presidio nel caso in cui, ricorrendo i presupposti di proporzionalità, si optasse per una soluzione di convergenza. Tali informazioni costituirebbero peraltro l'utile supporto al processo decisionale che interesserà gli Organi Aziendali nella scelta dell'assetto organizzativo.

2. Programmazione e rendicontazione dell'attività di controllo

Pag. 16: <<*In particolare: le funzioni di conformità alle norme e di controllo dei rischi presentano annualmente agli organi aziendali, ciascuna in base alle rispettive competenze, un programma di attività, in cui sono identificati e valutati i principali rischi a cui la banca è esposta e sono programmati i relativi interventi di gestione. La programmazione degli interventi tiene conto sia delle eventuali carenze emerse nei controlli, sia di eventuali nuovi rischi identificati;*>>.

La previsione normativa in questione definisce degli obblighi fondati su principi di funzionamento mutuati dalla Revisione Interna (ed estesi in questi primi anni quale prassi operativa alla Funzione di Conformità) non tenendo invece conto delle diversità che contraddistinguono la modalità di espletamento dell'attività di risk management. La Revisione Interna di norma opera definendo un piano di attività con copertura

evidentemente parziale per ciascun ciclo di gestione delle diverse aree di processo e rischio ed in esito alle stesse produce *deliverable* per ciascun task di piano consuntivabili in modo naturale in una relazione complessiva di fine ciclo. La copertura completa delle aree di processo e di rischio si realizza di norma in un orizzonte pluriennale.

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

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

Pag. 17: *<<Al termine del ciclo gestionale, con cadenza quindi annuale, le funzioni aziendali di controllo: - presentano agli organi aziendali una relazione dell'attività svolta, che illustra le verifiche effettuate, i risultati emersi, i punti di debolezza rilevati e propongono gli interventi da adottare per la loro rimozione; - riferiscono, ciascuna per gli aspetti di rispettiva competenza, in ordine alla completezza, adeguatezza ed affidabilità del sistema dei controlli interni.>>.*

Con riferimento alla funzione di internal audit tale formulazione non appare coerente con l'impostazione secondo cui a fronte delle carenze riscontrate non vengono definiti (o anche solo proposti) direttamente a cura della revisione interna, gli interventi correttivi da adottare bensì vengono solo fornite delle "raccomandazioni" al fine di perseguire un più adeguato assetto dei controlli e presidio del rischio. L'identificazione delle azioni correttive è attività propria dell'organo con funzione di gestione. La formulazione, peraltro, va allineanata con quanto specificato, invece, a pag. 20 ossia "*la funzione di revisione interna (internal audit) ... omissis ... sulla base dei risultati dei propri controlli formula raccomandazioni agli organi aziendali*".

Con riferimento alla Risk Management Function (RMF), il ciclo di gestione (l'esercizio annuale per lo più) per le attività svolte e soprattutto per la relativa disclosure agli Organi Aziendali rappresenta solo una segmentazione convenzionale rispetto alla quale è utile (peraltro propedeutica ad obblighi di disclosure istituzionale) riepilogare "istituzionalmente" gli esiti delle attività svolte alla fine del periodo di riferimento. La suddetta convenzione "amministrativa" tuttavia non deve, a nostro avviso, attenuare la maggiore rilevanza assunta dall'informativa continuativa periodica in esito all'attività svolta nel continuo dalla RMF e che costituisce la base per un consapevole processo decisionale, anche esso continuo, al cui vertice figurano gli Organi Aziendali. Si richiede pertanto che, nel passaggio in questione della Proposta di

Disciplina, con riferimento alla RMF, siano maggiormente specificati ed esaltati gli obblighi informativi di carattere periodico verso gli Organi Aziendali, propedeutici al processo decisionale, in luogo di una disclosure annuale a valenza riepilogativa e che nella sua estensione complessiva a tutte le aree presidiate rischia di essere nel tempo assimilata ad un formale adempimento amministrativo.

3. Requisiti specifici delle funzioni aziendali di controllo – 3.2 Funzione di conformità alle norme (Compliance)

Pag. 17 <<"*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 ripercussioni significative in termini di rischi operativi e di reputazione e conseguenti danni patrimoniali*" >>

La normativa fiscale ha un'indubbia rilevanza in valore assoluto per le implicazioni che ne discendono in occasione della violazione delle previsioni in esse contenute, ma in termini relativi è equivalente ad altri ambiti normativi non indicati nelle presenti disposizioni, quali a mero titolo di esempio, la sicurezza delle informazioni (ICT, Logistica, Dati).

La nota n. 20 *<< (20) Le banche devono altresì tener conto dei rischi derivanti dal coinvolgimento in operazioni fiscalmente irregolari poste in essere dalla clientela>>,* nell'attuale formulazione, potrebbe indurre confusione tra aree di competenza della Funzione di Compliance e la Funzione Aziendale Antiriciclaggio.

Si riterrebbe altresì opportuno circoscrivere il perimetro normativo in capo alla Funzione Compliance: il governo delle normative e la previsione e neutralizzazione dei rischi richiedono un coordinamento tra l'azione di traduzione delle medesime norme in regole operative e le attività poste in essere dalle strutture della Banca. La scelta di accentramento delle responsabilità, che deriva dalla lettura del documento in consultazione, risulta di difficile attuazione rispetto ad articolazioni organizzative sempre più complesse e, ormai, specializzate nell'ambito delle competenze a loro assegnate tale da pregiudicarne anche la velocità di attuazione delle azioni di adeguamento, tempo per tempo, introdotte dal legislatore; in altri termini, rispetto all'ipotesi di estendere indefinitamente il perimetro normativo della Funzione di conformità si riterrebbe opportuno circoscrivere meglio il campo di applicazione delle norme da attribuire alla Funzione di Compliance, ferma restando la necessità di veicolare alla stessa, da parte di tutte le strutture aziendali, le opportune informazioni utili a determinare la complessiva situazione della gestione del rischio di non conformità.

3. Requisiti specifici delle funzioni aziendali di controllo – 3.3 Funzione di controlli dei rischi (risk management function)

Pag. 20: <<*La funzione di controllo dei rischi: dà pareri preventivi sulla coerenza con la politica di governo dei rischi delle operazioni di maggiore rilievo>>.*

È necessario che sia chiarito l'intendimento dell'Organo di Vigilanza sul ruolo da assegnare alla RMF nel processo di assunzione dei rischi. In tale ambito infatti si concretizzano le operazioni di maggior rilievo secondo un consolidato iter procedurale che, in via semplificata, è costituito dalle principali fasi di valutazione istruttoria della controparte e dell'operazione nel suo complesso, delibera, perfezionamento. Le operazioni di maggior rilievo, così come ogni altra operazione "ordinaria" aziendale, vengono effettuate all'interno del *framework* di policy (e processi), limiti e deleghe che la stessa RMF ha contribuito a definire. Il rispetto della "Regolarità Operativa" presuppone che ogni operazione sia effettuata all'interno di tale *framework*, evidentemente definito dall'Organo con Funzione di Gestione ed approvato dall'Organo con Funzione di Supervisione Strategica. Ogni operazione con caratteristiche non riconducibili al suddetto *framework* (per importo, forma tecnica, canale di provenienza, segmento di business al quale è rivolta, struttura contrattuale, modalità di perfezionamento, ecc.) deve naturalmente essere sottoposta ad autorizzazione dell'Organo con Funzione di Supervisione Strategica in analogia a quanto previsto per ogni nuovo prodotto e servizio.

Tutto ciò premesso si riportano di seguito alcune ipotesi interpretative rispetto alle quali si richiede sia chiarito l'intendimento della Vigilanza:

1) Il parere preventivo è assimilabile, costituendone di fatto l'esito, ad una valutazione istruttoria della controparte e dell'operazione ed è dunque riferito al "merito" della stessa. In via attuativa l'esame istruttorio che precede la formulazione del parere può essere svolto autonomamente od utilizzando, con eventuali opportune integrazioni, l'esito dell'attività svolta dalla funzione proponente (di norma depositaria del complessivo materiale istruttorio). Indipendentemente dalla modalità con cui viene condotta l'analisi da parte della RMF, gli esiti della stessa definiscono la posizione della funzione circa l'opportunità di assumere il rischio che l'operazione comporta date le sue complessive caratteristiche (ed in tal ottica pare non razionale una valutazione riferibile alla sola rischiosità non tenendo in debita considerazione il rendimento ad essa associato).
2) Il parere preventivo è riferito alla "conformità" (quale sinonimo attuativo del concetto di coerenza) dell'operazione alle Policy (e processi), ai Limiti ed alle Deleghe che costituiscono il complessivo framework di assunzione dei rischi. Si tratterebbe in tal caso dell'esercizio in chiave preventiva della consueta prerogativa della Revisione Interna di verifica della Regolarità Operativa posto, peraltro, che trattandosi di operazioni di maggior rilievo (comunque le stesse siano definite) sono di norma assoggettate ad organi deliberanti di elevato standing i quali evidentemente sono anche responsabili diretti della "conformità" dell'operazione stessa (così come ogni organo deliberante per ogni tipo di operazione).
3) Il parere preventivo è richiesto, in analogia a quanto previsto per i nuovi prodotti e servizi, con riferimento alle sole operazioni le cui caratteristiche si discostano (per importo, forma tecnica, canale di provenienza, segmento di business al quale è rivolta, struttura contrattuale, modalità di perfezionamento, ecc.) da quanto previsto dal framework di assunzione rischi, che come tali debbono essere sottoposte ad autorizzazione dell'Organo con Funzione di Supervisione Strategica o all'Organo con Funzione di Gestione in presenza di deleghe a specifiche deroghe.

Si ravvisano nelle prime due ipotesi forti criticità il cui impatto si ritiene debba essere attentamente valutato dall'Organo di Vigilanza:

- Nella prima ipotesi si richiama un rischio di sovrapposizione con istituti quali l'Istruttoria di Secondo Livello di norma presenti nei processi aziendali, ed in particolare per le operazioni di maggior rilevanza. Si sollevano peraltro perplessità sul fatto che l'esercizio di tale prerogativa da parte della RMF ne farebbe conseguire un naturale coinvolgimento della stessa nel processo di assunzione dei rischi con riferimento ad una singola operazione e non, come invece si ritiene opportuno, con riferimento alla "tenuta" del complessivo *framework* di assunzione dei rischi.
- Nella seconda ipotesi il ruolo esercitato appare:
    a. ridondante in un contesto in cui il *framework* di assunzione dei rischi sia stato opportunamente definito, internamente normato ed operativamente ed organizzativamente implementato;
    b. incoerente con la mission dei controlli di secondo livello (cfr. anche quanto precisato proprio nel documento in analisi sulla funzione di Conformità) che non prevede un ruolo di verifica della regolarità operativa. Ove anche si considerasse un'eccezione il circoscritto ambito delle operazioni di maggior rilievo si tenga comunque conto che alla rilevanza dell'operazione è di norma associata la rilevanza dell'Organo Deliberante, le cui prerogative di controllo diretto sulla conformità dell'operazione alle policy aziendali si ritiene debbano essere rimarcate nella Proposta di Disciplina.

In conclusione si chiede di valutare una proposta alternativa di previsione normativa per la RMF di verifica obbligatoria e riesame ex-post delle operazioni di maggior rilievo quale task:

- da inserire in un contesto di controllo della qualità del processo del credito (o del processo di investimento per estendere l'ambito all'operatività finanziaria) propedeutico al tuning evolutivo/correttivo del framework di assunzione dei rischi, che rappresenta a nostro avviso, una delle principali attribuzioni della RMF,
- che rappresenti un fattore di monito e richiamo alla massima attenzione verso gli attori direttamente coinvolti nel processo di assunzione rischi (dal contatto commerciale, al perfezionamento amministrativo passando per istruttori e organi deliberanti).

Pag. 19: <<*Al fine di rafforzarne l'indipendenza, il responsabile della funzione* (di controllo dei rischi) *può essere collocato alle dirette dipendenze del comitato controllo e rischi, ove costituito, o dell'organo con funzione di supervisione strategica (22). (22) Le banche classificate, a fini SREP, nelle macro-categorie 1 e 2 (cfr. Circolare 269 del 7 maggio 2008, "Guida per l'attività di vigilanza", Sezione I, Capitolo I.5) collocano obbligatoriamente la funzione di controllo dei rischi alle dirette dipendenze del comitato controllo e rischi, ove costituito, o dell'organo con funzione di supervisione strategica*>>.

Nella declinazione organizzativa delle responsabilità della RMF si ritiene di primaria importanza che tale funzione oltre a sviluppare metodologie e modelli di misurazione e valutazione dei rischi:

- concorra alla definizione ed allo sviluppo del *framework di assunzione e gestione dei rischi*, assicurando che lo stesso sia conforme alle normativa di riferimento, allineato alle best practice di mercato e funzionale al contesto gestionale interno (posto che il *framework di assunzione e*

gestione dei rischi è costituito dai presidi organizzativi, dai processi e dai controlli di linea, dagli strumenti, dalle policy, dalle metodologie e dai criteri di valutazione dei rischi);

- monitori l'andamento delle attività (e delle passività) a rischio in relazione all'andamento dei mercati di riferimento ed al funzionamento del sistema di gestione interno ed in tale ambito:
    - effettui attività di controllo di secondo livello sull'adeguatezza, l'efficacia e la tenuta nel tempo del *framework di assunzione e gestione dei rischi* ,
    - rilevi eventuali situazioni di rischio eccedenti i limiti definiti dalle policy interne e dalla normativa esterna e, più in generale, situazioni potenzialmente dannose o sfavorevoli al fine di sottoporle al processo decisionale per una valutazione degli interventi mitigativi da porre in essere
    - identifichi necessità di fine tuning / manutenzione correttiva ed evolutiva del framework di assunzione e gestione dei rischi fornendo un supporto, per quanto di competenza, nella implementazione dei relativi interventi.

È altresì irrinunciabile che la stessa funzione, anche in esito alle attività di monitoraggio svolte, riferisca, oltre che all'Organo con Funzione di Gestione, obbligatoriamente e in via diretta anche all'Organo con Funzione di Supervisione Strategica in merito all'andamento dei rischi nei diversi comparti operativi e di business supportando gli stessi Organi nella definizione degli orientamenti strategici e delle politiche di rischio e nella relativa attuazione.

Ciò premesso, si ritiene che nell'esercizio delle suddette prerogative la RMF, nell'ambito dell'organizzazione aziendale, sia il principale referente in materia di rischi dell'Organo con Funzione di Gestione ed allo stesso tempo svolga per detto Organo un "ruolo di garanzia" nell'interlocuzione e nell'iterazione ordinaria con le strutture operative e di business: l'indipendenza della RMF dalle strutture operative e di business le consente di esercitare tale ruolo concretizzando in tal modo il concetto di "funzione di controllo di secondo livello" ed allo stesso tempo assicurando l'efficacia dell'azione in quanto parte integrante della complessiva fase esecutiva. In modo analogo la Revisione Interna svolge lo stesso "ruolo di garanzia" verso l'Organo con funzione di Supervisione Strategica: l'indipendenza della Revisione Interna dall'Organo con funzione di Gestione e quindi dalla complessiva fase esecutiva della quale fanno parte sia le strutture operative e di business sia le funzioni di controllo di secondo livello le consente di esercitare tale ruolo concretizzando in tal modo il concetto di "funzione di controllo di terzo livello" ed allo stesso tempo assicurando l'efficacia dell'azione in quanto committed dall'Organo con funzione di Supervisione Strategica.

Ad ulteriore supporto delle argomentazioni sopra rappresentate si ritiene che il principio dell'efficacia dell'azione delle Funzioni di Controllo debba assumere, in un contesto di evoluzione della disciplina in materia di controlli ed alla luce dei riscontri degli ultimi anni, primaria rilevanza. L'efficacia è strettamente collegata all'integrazione della RMF nella organizzazione aziendale richiamando un concetto di *risk management* quale processo aziendale che coinvolge, in una logica sia top-down sia bottom-up, tutta la struttura: unità commerciali, funzioni di controllo, manager, organi di vertice.

La collocazione organizzativa della RMF a tal proposito costituisce il principale fattore di successo od insuccesso della Funzione dal punto di vista dell'efficacia della sua azione. L'eccessiva distanza, al limite indipendenza, dalla fase esecutiva, eventualmente attenuata da un coinvolgimento formale in momenti istituzionali, che si avrebbe riportandola alle dirette dipendenze dell'Organo con Funzione di Supervisione Strategica, ne attenuerebbe, a nostro parere, il sostanziale apporto e contributo per una assunzione e

gestione dei rischi sempre più ponderata e consapevole sviluppato all'interno di una fase esecutiva al cui vertice figura l'Organo con Funzione di Gestione.

Si richiede pertanto che per la RMF sia prevista la possibilità, indipendentemente dalla classe SREP di appartenenza, di poter collocare la funzione alle dirette dipendenze dell'Organo con Funzione di Gestione. Sul punto è altresì necessario, anche tenendo conto di quanto evidenziato nel presente documento circa l'assenza di una circostanziata previsione di ruolo da parte del Direttore Generale nel Sistema dei Controlli Interni, prevedere la possibilità di identificare il Direttore Generale, "in quanto vertice della struttura interna e partecipante alla funzione di gestione", quale referente diretto della RMF e più in generale delle funzioni rientranti nell'ambito dell'area dei controlli di secondo livello.

In ultimo si rappresenta che pare non coerente la collocazione organizzativa indicata con quanto previsto nello stesso schema di disciplina in materia di nomina e revoca dei responsabili delle Funzioni di Controllo: Capitolo 7, Sezione 3, paragrafo 1 <<*i responsabili siano nominati e revocati (motivandone le ragioni) dall'organo con funzione di gestione, d'accordo con l'organo con funzione di supervisione strategica, sentito l'organo con funzione di controllo.*>>

3. Requisiti specifici delle funzioni aziendali di controllo – 3.4 Funzione di revisione interna (Internal Audit)

Pag 21: << *il grado di autonomia (della funzione di revisione interna) può essere accresciuto con la collocazione alle dirette dipendenze del comitato controllo e rischi, ove costituito, o dell'organo con funzione di supervisione strategica (obbligatorio per le banche in macrocategoria 2). 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*>>

Tale formulazione non appare sufficientemente chiara, potendo essere interpretata in due modi distinti:

a) possibilità, per la Direzione Generale (o dell'Organo con Funzione di Gestione) di "indirizzare il piano annuale delle attività" (chiedendo, ad esempio, alla funzione di audit di verificare una determinata fattispecie operativa o un determinato processo); in tal caso l'azione della Direzione è finalizzata ad indirizzare il Piano di attività solo per 'oggetto';

b) possibilità, per la Direzione Generale (o dell'Organo con Funzione di Gestione) di "indirizzare" i singoli interventi di revisione, stabilendo, ad esempio, particolari oggetti o i tempi delle verifiche e le modalità di esecuzione dell'incarico.

Si ritiene chiarire meglio tale aspetto in relazione alla necessità di circostanziare meglio il grado di indipendenza proprio della Funzione di Revisione interna.

Pag. 21: <<- *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.*>>

Si evidenzia che ad oggi non risulta sussistere un parallelo obbligo di condivisione con la Revisione Interna delle proprie evidenze da parte delle Società di Revisione (mentre è prassi il contrario). L'applicazione della norma, pertanto, potrebbe essere condizionata dalla riformulazione in tal senso degli accordi contrattuali con le società di revisione, ovvero, dall'esplicito obbligo di condivisione in sede normativa.

3. Requisiti specifici delle funzioni aziendali di controllo – 3.5 Rapporti tra le funzioni aziendali di controllo e altre funzioni aziendali

Pag. 22: <<*Tenuto conto delle forti interrelazioni tra le diverse funzioni aziendali di controllo, specie tra le attività di controllo di conformità alle norme, di controllo dei rischi operativi e di revisione interna, è necessario che i compiti e le responsabilità delle diverse funzioni siano comunicati all'interno dell'organizzazione aziendale, in particolare per quanto attiene alla suddivisione delle competenze relative alla misurazione dei rischi, alla consulenza in materia di adeguatezza delle procedure di controllo nonché alle attività di verifica delle procedure medesime.*>>

Si propone di modificare il testo nel seguente modo: " *Tenuto conto delle forti interrelazioni tra le diverse funzioni aziendali di controllo, specie tra le attività di controllo di conformità alle norme, di controllo dei rischi operativi e di revisione interna, è necessario che i compiti e le responsabilità delle diverse funzioni* **siano formalizzati, se opportuno, anche mediante accordi di servizio** *e comunicati all'interno dell'organizzazione aziendale, in particolare per quanto attiene alla suddivisione delle competenze relative alla misurazione dei rischi, alla consulenza in materia di adeguatezza delle procedure di controllo nonché alle attività di verifica delle procedure medesime.*

Sezione IV – Esternalizzazione di funzioni aziendali (outsourcing)

1. Principi generali e requisiti particolari

Pag. 23: << *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.*>>

Si ritiene che in termini generali debba essere specificata la non applicabilità delle disposizioni contenute In questa sezione ai casi di esternalizzazione infragruppo, con ciò distinguendo fra generiche iniziative di esternalizzazione ("outsourcing") e riallocazione di funzioni e competenze nell'ambito del medesimo gruppo di società ("accentramento"). Quest'ultima fattispecie, riferita alla riallocazione di attività su una o più società appartenenti ad un medesimo gruppo, appare ricadere nella disciplina generale del gruppo bancario per la quale "viene lasciata all'imprenditore la scelta dell'assetto organizzativo e patrimoniale che meglio risponda ai suoi obiettivi gestionali" [1] . La Capogruppo stessa, accomunando le società del gruppo in un comune disegno imprenditoriale e sottoponendole a direzione unitaria perseguirà, anche nell'interesse dell'azionista, obiettivi di efficienza complessiva nelle scelte di esternalizzazione infragruppo che appaiono

[1] Banca d'Italia – Istruzioni di Vigilanza per le banche, Titolo I, Capitolo 2, Sezione I

condivisibili e chiaramente rappresentati nell'ipotesi normativa. Rileva da ultimo, in coerenza con le prerogative attribuite alla Capogruppo in materia di coordinamento e controllo dell'efficiente allocazione delle attività infragruppo, l'ulteriore ruolo di quest'ultima per l'esecuzione delle istruzioni impartite dall'Organo di vigilanza che va dall'emanazione di disposizioni alle proprie società a quello di referente della Banca d'Italia in materia di vigilanza consolidata.[2]

In termini specifici il permanere di adempimenti a carico della banca dell'obbligo di mantenimento delle competenze tecniche sulla materia esternalizzata sembra condizionare in modo significativo le scelte *make or buy* della banca stessa a sfavore dell'esternalizzazione. In tale fattispecie infatti la banca committente sarebbe chiamata a tenere su di sé una parte significativa dei costi di mantenimento ed aggiornamento delle strutture tecniche, accettando peraltro il rischio che tali strutture, necessariamente lontane dagli accadimenti operativi di maggiore dettaglio, possano progressivamente perdere esperienza professionale diretta sulla materia esternalizzata. Appare prevedibile altresì che l'adempimento possa, per alcune casistiche, far propendere la banca per la rinuncia all'esternalizzazione ovvero per la re-internalizzazione di attività già esternalizzate, ciò per effetto dei maggiori costi e rischi sopra evidenziati.

Risultati analoghi, con minore impatto diretto, si potrebbero ottenere attraverso la prescrizione di dover obbligatoriamente disporre/predisporre, in caso di esternalizzazione (outsourcing) di funzioni aziendali rilevanti, di/un adeguato Piano volto ad assicurare la Continuità Operativa delle Funzioni interessate in caso di mancata erogazione del servizio da parte dell'outsourcer.

Pag. 24: <<*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").*>>

L'ipotesi esposta di non applicabilità all'ambito infragruppo delle prescrizioni sull'esternalizzazione si conferma con gli ulteriori contenuti di pag. 24. Si consideri infatti che in ambito di gruppo il conflitto di interesse dell'outsourcer si presume neutralizzato dall'esercizio del ruolo di indirizzo e coordinamento della Capogruppo la quale, esercitando anche le sue prerogative di controllo provvederebbe anche alla verifica del rispetto delle aspettative di complessiva efficienza della collaborazione. I compiti di controllo a carico del committente potrebbero in tale ambito risultare residuali e comunque non necessitare di uno specifico profilo di referente per le attività esternalizzate.

Anche per quanto attiene ad esternalizzazioni (extragruppo se riferite ai gruppi bancari) su iniziativa della banca, la figura di uno specifico referente può presentare profili di ridondanza, sia per la presenza di

[2] Cfr. nota 1

responsabilità organizzative generalizzate già efficaci in questo ambito[3] sia per la variabilità di presidio richiesta dai rapporti di esternalizzazione, eterogenei fra loro per connotato strategico e/o contenuto operativo. Si richiede pertanto di restringere tale prescrizione ad ambiti di fabbisogno meglio individuabile lasciando nel contempo alla Banca la prerogativa di *"nominare un referente, laddove ritenuto opportuno o necessario".*

Pag. 25: << *Entro il 30 aprile di ogni anno le banche trasmettono alla Banca d'Italia una relazione, redatta dalla funzione di revisione interna - o, se esternalizzata, dal referente aziendale - con le considerazioni dell'organo con funzione di controllo e approvata dall'organo con funzione di supervisione strategica, relativa ai controlli svolti sulle funzioni operative importanti esternalizzate, alle carenze eventualmente riscontrate e alle conseguenti azioni correttive adottate.*>>

Si ravvisa la necessità di precisare meglio gli ambiti di detta Relazione annuale da parte della Revisione Interna, tenendo conto che gli obblighi di valutare l'adeguatezza delle altre Funzioni di Controllo (benchè non sempre e prescrittivamente su base annuale su tutte le funzioni di controllo) sono già incardinati in seno alla Revisione interna, con periodicità che definisce l'azienda e a prescindere dall'esternalizzazione o meno delle stesse.

Sezione V – Il sistema dei controlli interni nei gruppi bancari

2. Controlli interni di gruppo

Pag. 28: <<*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 (*Esternalizzazione di funzioni aziendali*), ai seguenti criteri:*>>.

L'accentramento presso la Capogruppo delle Funzioni di Controllo costituisce una scelta di governance che contestualmente vuole perseguire i) una maggiore efficienza interna al Gruppo, ii) l'efficacia dell'azione di controllo attraverso la creazione di centri di competenza specialistici in materia, iii) la costituzione di un presidio unitario dei rischi che fornisca concreta attuazione del principio di responsabilità della stessa Capogruppo, ferme restando le responsabilità individuali degli Organi Aziendali delle Società Controllate in materia di assunzione, gestione e controllo dei rischi.

Le caratteristiche attuative di tale scelta di governance, anche in termini di attività, responsabilità ed attribuzioni, modalità di espletamento, rappresentazione e diffusione degli esiti, relazione/rapporto con gli Organi Aziendali della Società Controllata, governance operativa della Funzione sono di norma disciplinate nel Regolamento di Corporate Governance del Gruppo Bancario. Detto regolamento, a nostro parere, assolve integralmente gli obblighi di disciplina dell'esercizio delle Funzioni di Controllo presso la

[3] Si pensi ad esempio, alla Funzione di Revisione Interna, sull'efficacia della quale insistono compiti e responsabilità di controllo diffuse (CDA, Comitato Controlli e Collegio Sindacale)

Capogruppo e le Società Controllate unitamente ai Regolamenti interni aziendali che recepiscono e definiscono compiti, ruoli e responsabilità delle Funzioni di Controllo accentrate presso la Capogruppo.

Il ricorso alla formalizzazione di un contratto tra le parti si ritiene utile in una logica di ripartizione dei costi e dunque di definizione dei corrispettivi economici in capo a ciascun componente del Gruppo, ritenendolo altresì non necessario nei casi non sussistano presupporti o esigenze di tale natura.

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

Si ritengono pertanto, nei casi di accentramento delle Funzioni di Controllo presso la Capogruppo, non adeguati i riferimenti specifici alle previsioni della Sezione IV. Ad esempio non si tiene in debito conto, a nostro parere:

- l'intrinseco interesse della Capogruppo a fornire servizi adeguati e in linea con i principi esposti nella Sezione 4 (livelli di servizio, competenza, tempestività nell'informazione, sicurezza, ecc.) ;
- il principio di efficienza alla base della scelta di accentramento: anti economicità del riferimento specifico al referente interno, al mantenimento delle competenze in una logica di complessivo assetto del Sistema dei Controlli Interni di Gruppo;
- la tipologia di relazione Capogruppo-Controllata e le regole di Governance del Gruppo Bancario con riferimento :
    - ad eventuali clausole risolutive per impossibilità, incapacità o mancato rispetto dei livelli di servizio,
    - ad un obbligo di controllo e quindi di relazione degli esiti da parte dalla funzione di revisione interna - o, se esternalizzata, dal referente aziendale – che non sia riconducibile al normale assoggettamento di tutte le funzioni aziendali al controllo della revisione interna esercitato su base individuale o a livello consolidato secondo le previsioni in materia di "Controlli interni di Gruppo", Sez. 5, paragrafo 2.

Tutto ciò premesso si richiede:

- di sostituire il riferimento alla Sezione IV con specifiche previsioni / obblighi delle Funzioni accentrate verso gli Organi Aziendali delle Società Controllate;
- di prevedere in tale ambito che l'obbligo per le Società Controllate di individuare, all'interno della propria organizzazione, un responsabile del controllo della singola funzione di Controllo accentrata presso la Capogruppo, sia lasciato all'autonomia della capogruppo trasformando l'obbligo in possibilità ove ciò sia ritenuto opportuno per assicurare la massima funzionalità del sistema dei controlli e che tale previsione sia assolvibile anche attraverso l'attribuzione di tale responsabilità alla Direzione Generale della stessa Società Controllata.

Pag. 28: <<- *devono essere chiaramente valutati e documentati i costi, i benefici ed i rischi alla base della soluzione adottata; tale analisi deve essere periodicamente aggiornata;* >>

Come sopra cennato, nel caso di esternalizzazione alla Capogruppo tali profili si ritiene siano già intrinsecamente valutati attraverso gli ordinari compiti di monitoraggio (di efficace ed efficiente funzionamento delle funzioni di controllo esternalizzate alla Capogruppo) svolti dai CDA delle Controllate e della Capogruppo stessa. Una 'formale' verifica in tal senso nulla aggiungerebbe stante - come detto - l'interesse della Capogruppo stessa a fornire servizi adeguati anche sotto il profilo del presidio di tutti i rischi. Le logiche, poi, di accentramento possono non necessariamente - consapevolmente, in funzione del complessivo modello di controllo e sotto la responsabilità della Capogruppo - rispettare pariteticamente alcuni di questi criteri: in tali casi non si capisce come possano rilevare le valutazioni (anche periodiche) della Controllata bancaria. Si chiede, in ogni caso, di chiarire che tale valutazione di costi, benefici e rischi spetti solo alla Capogruppo e sia ascrivibile alla sola sua esclusiva responsabilità.

Pag. 28: <<- *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 (26);*>>

La formulazione (che, di fatto, reintroduce una componente "decentrata" di controllo) non appare adeguata per rappresentare la realtà di tutti i gruppi bancari. Si ritiene, pertanto, che sia più opportuno lasciare l'opportunità di istituire detti 'referenti' ad una valutazione dell'intermediario (in caso di accentramento delle Funzioni, alla sola Capogruppo) in funzione del numero di controllate o delle filiali territoriali , complessità dei business gestiti e esigenze di presidio nel continuo, esistenza di controlli a distanza ecc.). Tale soluzione potrebbe generare ulteriori inefficienze di interfacciamento con le controllate specie nei contesti di Gruppo nei quali, l'operatività delle Funzioni di Controllo, funziona in via ordinaria senza bisogni dei referenti interni, potendo contare - in caso di problemi - dell'ordinaria interlocuzione con la Direzione Generale o con gli Organi di Controllo per la risoluzione degli stessi. Da ultimo si ravvisano non pochi ostacoli giuslavoristici nell'attuale normativa (ad es. nell'istituto del 'distacco') per la realizzazione di una dipendenza 'gerarchica', oltre che quella funzionale.

Pag. 28: <<- *qualora l'esternalizzazione sia effettuata alla capogruppo, all'interno della funzione di revisione interna della stessa viene mantenuta un'adeguata separazione tra le unità e le risorse deputate a svolgere l'internal audit su base individuale per le controllate da quelle responsabili dei controlli su base consolidata le quali, tra i diversi compiti, hanno anche quello di verificare la funzionalità del complessivo sistema dei controlli interni di gruppo.*>>

La formulazione appare impattare immotivatamente sulla realizzazione delle sinergie derivanti dall'effettuare attività sia a valere della capogruppo sia a valere delle controllate pur nel rispetto di procedure interne atte a disciplinare/gestire eventuali conflitti d'interessi. Ciò, parrebbe essere stato disciplinato, in prima istanza, al principale fine – raggiungibile ed accertabile in modo meno oneroso, come spesso effettuato, nella nostra esperienza, anche in sede ispettiva dell'Organo di Vigilanza – di più agevolmente accertare l'adeguatezza quali-quantitativa dei team assegnati alle diverse società. Quanto

sopra, ferme restando le considerazioni già formulate, circa l'interesse della Capogruppo a fornire comunque servizi quali quantitativamente adeguati.

Qualora poi l'obiettivo della prescrizione sia il contenimento dei potenziali conflitti di interesse fra le risorse assegnate alle diverse società si rammenta che gli stessi sono già gestiti, ad esempio, con le procedure QAR per le funzioni di revisione interna certificate. Sarebbe quindi sufficiente - ed in linea con l'importanza che la certificazione assume nella documentazione di Basilea più recente sulla Revisione Interna - escludere tali obblighi di separatezza per le funzioni accentrate presso la Capogruppo e con processi certificati per la 'gestione dei conflitti di interesse'.

Sezione VII – Procedure di allerta interna

Pag. 31: <<*Le procedure di allerta interna stabiliscono, in particolare: le modalità attraverso cui segnalare eventuali criticità individuate e i soggetti che devono essere informati;*>>

Si riterrebbe opportuno integrare la previsione normativa con esplicita richiesta agli intermediari di individuazione di una struttura di ultimo livello per l'indirizzamento e valutazione - di prima istanza - circa la fondatezza delle segnalazioni e, soprattutto, le azioni più adeguate da intraprendere.

Pag. 31: <<*Le procedure devono garantire in ogni caso la riservatezza e la protezione dei dati personali del soggetto che effettua le segnalazioni e del soggetto eventualmente segnalato*.>>

L'attuale formulazione lascerebbe intendere anche la protezione di soggetti che segnalano 'fenomeni infondati' verso i quali invece l'azienda deve, invece, poter reagire. Senza una adeguata disciplina di tali aspetti, la previsione nell'attuale formulazione si presta a bloccare 'ab origine' qualsiasi intervento disciplinare, potendo, in teoria, il dipendente - appena effettuata la contestazione disciplinare - effettuare una segnalazione infondata, invocando il sistema di "protezione".

Sezione IX – Informativa alla Banca d'Italia

Pag. 33: << *Nel caso di gruppi bancari, inoltre, le rispettive capogruppo coordinano e trasmettono alla Banca d'Italia, per tutte le banche del gruppo, la stessa documentazione richiesta nel caso delle banche non appartenenti a gruppi bancari. Le relazioni sulle attività svolte dalle funzioni aziendali di controllo della capogruppo contengono anche gli esiti delle verifiche effettuate, dei risultati emersi, dei punti di debolezza rilevati con riferimento, oltre che alla capogruppo medesima, anche al gruppo bancario nel suo complesso e descrivono gli interventi da adottare per la rimozione delle carenze rilevate.*>>

Si ritiene opportuno prevedere – specie nel caso di funzioni accentrate - l'invio di un'unica relazione che rappresenti il contenuto delle attività svolte a valere su ciascuna società controllata nonché sulla Capogruppo, evidenziando, quindi, sia gli aspetti di criticità relativi ad una specifica società sia gli effetti sul gruppo nel suo complesso. Tale prescrizione risulterebbe già in linea con le prescrizioni vigenti circa la relazione annuale della Capogruppo sul Sistema dei Controlli Interni, senza creare ulteriori oneri.

Capitolo 8 – Sistema Informativo

Sezione I – Disposizioni di Carattere Generale

1. Premessa

Pag. 44: <<*Le concrete misure da adottare possono essere individuate tenendo conto, oltre che degli specifici obiettivi strategici, anche, sulla base del principio di proporzionalità, delle dimensioni dell'intermediario, del tipo e della complessità della sua operatività, dal livello di automazione dei suoi processi e servizi*>>

Pag. 44: <<*In tale ambito, gli intermediari fanno riferimento agli standard e best practices definiti a livello internazionale in materia di governo, controllo e sicurezza dei sistemi informativi*>>

Su un piano generale, si esprime piena condivisione dei principi di indirizzo e delle connesse modalità di recepimento così come enunciati. Appare in particolare opportuno il riferimento al principio di proporzionalità. Parimenti utile appare il riferimento alle best practice quale criterio guida nella impostazione dei sistemi di governo e controllo.

L'adozione di best practices internazionali ha, come ovvio, riflessi di assoluto rilievo sull'organizzazione aziendale e, in qualche caso, sullo stesso modello di business. Conseguentemente, la piena efficacia di tale adozione non può prescindere dal progressivo conseguimento di successivi "livelli di maturità" organizzativa.

Quanto precede renderebbe quindi opportuno che il disposto normativo sia focalizzato su indirizzi strategici e su atti indispensabili per una consapevole assunzione dei rischi (cfr. Sez. III approvazione del rischio residuo), evitando nel contempo di richiamare nella normativa componenti anche importanti delle richiamate best practices che meritano però di essere declinate in base al più generale principio di proporzionalità e di "capability level" organizzativo.

2. Fonti normative

Pag. 45: In chiusura del paragrafo si afferma che nella successiva regolamentazione <<*si tiene anche conto dei seguenti documenti pubblicati da organismi internazionali:*>>

In tale ambito, per evitare di far considerare esaustiva la lista di standard che segue e rafforzare la generale valenza del principio affermato al primo paragrafo circa l'opportunità di fare "*riferimento agli standard e best practices definiti a livello internazionale*", si riterrebbe opportuno riformulare la riferita affermazione in "*… si tiene anche conto dei documenti pubblicati da organismi internazionali fra cui quelli di seguito indicati a mero titolo esemplificativo*:…"

4. Definizioni

Si riterrebbe opportuno inserire, fra le definizioni presenti nel paragrafo, anche quella di "incidente di sicurezza" in effetti inclusa nel successivo paragrafo "La gestione degli incidenti di sicurezza" a pag. 55 secondo cui "*Per incidente di sicurezza si intende ogni evento che implica la violazione o l'imminente minaccia di violazione delle norme e delle prassi aziendali in materia di sicurezza delle informazioni (ad esempio frodi informatiche, attacchi attraverso Internet nonché gravi malfunzionamenti e disservizi)…*".

Sezione II – Governo e organizzazione dell'ICT

1. Compiti dell'Organo con funzione di supervisione strategica

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

2. Compiti dell'Organo con funzione di gestione

L'asserzione secondo cui l'Organo di gestione *"… disegna e segue l'implementazione dei processi di gestione dell'ICT …*" appare meritevole di una riformulazione, da un lato finalizzata ad evitare che una impropria interpretazione del termine "*.. disegna …*" possa far attribuire all'Organo compiti esecutivi, dall'altro lato finalizzata a meglio distinguere il ruolo dell'organo di gestione dal ruolo del cosiddetto "*Direttore dei sistemi informativi*" (cfr. par. 3; com. 1; ali. 1).

L'asserzione secondo cui l'Organo con funzione di gestione "… *indipendentemente dall'articolazione organizzativa dell'intermediario e dalle strategie di sourcing adottata per l'ICT, … deve essere dotato di competenze tecnico – manageriali coerenti con le responsabilità ed i compiti menzionati.…*" appare di problematica applicazione ai contesti aziendali che adottano il modello c.d. tradizionale.

Circa la richiesta del box 4 secondo cui "…*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 …*", si segnala che lo standard ISO 27005 (gestione dei rischi nell'ambito 27001) si è già evoluto prevedendo un'integrazione con il framework di gestione dei rischi aziendali costituito dalla ISO 31000. Quest'ultimo prevede la possibilità che vi siano diverse "istanze" di gestione di rischi specifici, integrati attraverso la definizione comune di criteri e classificazioni di valutazione (impatti, scala dei rischi, criteri e modalità di accettazione e gestione dei rischi). Nel documento potrebbe essere richiamata una tale impostazione.

3. Organizzazione della funzione ICT

Pag. 49: <<*fermo restando quanto previsto nel Capitolo 7, Sezione III per le funzioni aziendali di controllo di secondo (controllo dei rischi e conformità alle norme) e terzo livello (revisione interna), l'attribuzione formale dei compiti di analisi del rischio informatico e di emanazione e verifica della policy di sicurezza ICT, da svolgere, nelle realtà più complesse, con personale con adeguate caratteristiche professionali e di specializzazione nella materia; va garantita l'indipendenza di giudizio rispetto alle funzioni operative*.>>

In effetti, l'ultimo capoverso, secondo cui va garantita l'indipendenza di giudizio della funzione preposta all'analisi dei rischi, potrebbe essere interpretato in modo estensivo giungendo a richiedere una separazione organizzativo-strutturale simile a quella richiesta per le funzioni di controllo di 2° e 3° livello.

Se ciò può risultare in linea di principio utile perché rafforza la "segregation of duty" non sembra però, né indispensabile (non trattandosi di una entità di controllo di 2° o 3° livello), né funzionale alle finalità dell'efficace esercizio della richiamata funzione.

Nel contempo, si sottolinea l'opportunità di prescrizioni finalizzate a garantire un tempestivo, completo e corretto flusso di informazioni dalle funzioni operative alla funzione sicurezza e da questa alla funzione rischi operativi.

Fermo restando quindi la finalità di "*garantire l'indipendenza di giudizio*" e di "*utilizzare per il compito personale con adeguate caratteristiche professionali*", si riterrebbe utile chiarire che tale "… *indipendenza di giudizio* …" non postula necessariamente l'adozione di misure separatezza organizzativo-strutturale quali quelle richieste per le funzioni di di controllo di 2° e 3° livello, ma richiede la piena garanzia di linee di riporto informativo che ne rafforzino l'indipendenza e l'efficacia.

Sezione III – La gestione del rischio informatico

Pag. 50: <<*Il processo di analisi deve essere svolto dall'utente responsabile con la partecipazione del personale tecnico, secondo una metodologia definita dall'organo con funzione di gestione*.>>

In tema, si osserva che l'assegnazione della primaria responsabilità di svolgimento dell'analisi all'utente, se da un lato ne garantisce la piena e proattiva partecipazione, dall'altro lato può portare a una incompleta identificazione/valutazione del rischio sotteso.

Tale formulazione pare peraltro incoerente con quanto riportato alla precedente pagina 49 (Sez. II, cap. 3) nella quale si dichiara che "*L'articolazione organizzativa della funzione ICT … contemplando in particolare … l'attribuzione formale dei compiti di analisi del rischio informatico … da svolgere, nelle realtà più complesse, con personale con adeguate caratteristiche professionali e di specializzazione nella materia; va garantita l'indipendenza di giudizio rispetto alle funzioni operative.*"

In aggiunta, si ritiene che l'attribuzione della responsabilità di eseguire l'analisi del rischio all'utente responsabile (come definito alla pagina 46 del documento di consultazione ["*utente responsabile (system owner)", la figura aziendale identificata o identificabile 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"]), possa introdurre i seguenti elementi di debolezza nell'analisi del rischio informatico:

- pluralità di "utenti responsabili" (una figura amministrativa per ogni sistema), che potrebbe determinare la necessità di "normalizzare" le rilevazioni a motivo delle inevitabili diverse sensibilità al rischio;
- sistemi non attribuibili ad un "utente", cioè ad una figura di natura amministrativa, in quanto sistemi di infrastruttura (apparati di telecomunicazione, elaboratori centrali, etc). come ovvio, tali sistemi richiederebbero specifiche analisi di rischio da parte di personale con adeguate conoscenze tecniche;
- rischi informatici non associabili a sistemi (applicazioni o infrastrutture) ma a processi (ad esempio il processo gestione delle modifiche all'infrastruttura o alle applicazioni) che, seppur oggetto delle prescrizioni di cui alla Sezione IV "Il sistema di gestione della sicurezza informatica", dovrebbero comunque rientrare nell'ambito della valutazione del rischio;

Si propone pertanto una diversa formulazione, che preveda l'obbligo di addivenire ad una:

- formale identificazione di "asset" aziendali (persone, informazioni, processi, software, sistemi, attrezzature, impianti) per ciascuno dei quali identificare un "proprietario" o "owner" (estendendo, con questo, il concetto di "system owner" introdotto nel documento);
- l'attribuzione ai proprietari degli asset del compito di svolgere l'analisi del rischio, con la partecipazione del personale tecnico;
- l'attribuzione al "Direttore dei sistemi informativi" della responsabilità finale dell'analisi (ciò in coerenza con quanto riportato alla precedente pagina 49 (Sez. II, cap. 3) nella quale si attribuisce a tale organo la garanzia dell'unitarietà del rischio informatico.

In ogni caso, si suggerisce di addivenire ad una soluzione che faccia prevalere, anche in ragione delle considerazioni sopra esposte circa i limiti della sola attribuzione all'utente delle responsabilità ascritte dalla norma, le logiche di processo testè enunciate ovvero, in alternativa, pur mantenendo un profilo cogente di stretta collaborazione dell'utente, ne attribuisca i compiti a specifiche funzioni (es. responsabile sicurezza) che favoriscano ex-ante l'esercizio del compito di riconduzione ad 'unitarietà' assegnato al Direttore dei Sistemi Informativi.

Pag. 50: << *in ogni caso deve essere determinato il rischio residuo da sottoporre ad accettazione formale dell'utente responsabile*>>

Sul punto potrebbe risultare opportuno esplicitare che, qualora il livello di rischio residuo eccedesse i limiti previsti per l'accettabilità da parte dell'utente responsabile, le misure di trattamento del rischio siano sottoposte all'attenzione dell'Organo con Funzione di Gestione.

Sezione IV – Il sistema di gestione della sicurezza informatica

2. La sicurezza dei dati e il controllo degli accessi

Pag. 53: << *la separazione degli ambienti di sviluppo, collaudo e produzione, con adeguata formalizzazione del passaggio di moduli software dal primo, al secondo, al terzo (par. 3), al fine di evitare l'accesso a dati riservati e sistemi critici da parte del personale addetto allo sviluppo e di esercitare un più stretto controllo degli accessi e delle modifiche nell'ambiente di produzione*>>

Premessa la piena condivisione dell'irrinunciabile principio di separatezza fra ambienti di sviluppo e produzione, si segnala l'opportunità di meglio circostanziarlo al fine di regolamentare situazioni in cui una parte ben identificata del personale di sviluppo svolga anche compiti di assistenza agli utenti e, nello svolgimento di tale attività, possa avere accesso all'ambiente di produzione.

3. La gestione dei cambiamenti

Pag. 53: << *la procedura di gestione dei cambiamenti – formalmente definita - è tesa a garantire un efficace controllo su modifiche, sostituzioni o adeguamenti tecnologici di sistemi e procedure nell'ambiente di produzione. Il processo deve svolgersi sotto la responsabilità di una figura o struttura aziendale con elevato grado di indipendenza rispetto alla funzione di sviluppo*>>

Sul punto si segnala l'opportunità di chiarire che per funzione di sviluppo si intende far riferimento sia alla funzione di sviluppo applicativo, sia di sviluppo della infrastruttura.

Sezione V – Il sistema di gestione dei dati

Si premette la piena condivisione e l'apprezzamento per l'inserimento nella regolamentazione di specifiche prescrizioni in tema "di gestione dei dati" sul quale, come riportato nel passo introduttivo, si fonda l'efficacia del sistema di governo dell'azienda.

Più in dettaglio, circa i "*requisiti che il sistema deve soddisfare*" (cfr. Com. 2°) si riterrebbe opportuno:

- precisare l'articolazione di ruoli e responsabilità richiesta al 3° alinea secondo cui "…*è definito uno standard aziendale di data governance, che individua ruoli e responsabilità delle funzioni coinvolte nel trattamento dell'informazione …*". La prevalente "forma elettronica" dei dati può, infatti, far ritenere il tema del trattamento e, in particolare, del controllo della qualità dei dati di mero interesse della funzione informatica condizionando in modo rilevante l'efficacia del sistema di "data governance". Si riterrebbe quindi opportuno, in sintonia con altri passi della norma (cfr. Sez. III "gestione del rischio informatico" comm. 2°, ruolo dell'utente responsabile) rafforzare la prescrizione completandola con "*… L'articolazione dei ruoli, ferma restando l'autonomia dei soggetti vigilati nella scelta delle forme organizzative a loro più adatte, deve riservare all'utente responsabile i compiti di governo delle regole di trattamento e di controllo sulla relativa osservanza …*"
- chiarire il 4° alinea secondo cui "*… l'utilizzo di procedure settoriali (contabilità, segnalazioni, antiriciclaggio, ecc.) non deve compromettere la qualità e la coerenza complessiva dei dati aziendali; a livello consolidato, va garantita l'integrazione tra le informazioni provenienti da tutte le componenti*

del gruppo … ". Si deve, infatti, ritenere che il tema che si intende sollevare non è quello dell'utilizzo di procedure settoriali ma quello della necessità di prevedere processi di alimentazione/controllo dei dati scambiati al fine di garantire "… *la qualità e la coerenza complessiva dei dati aziendali* …"

- chiarire la finalità del 6° alinea che - affermando che "*i dati devono essere conservati con una granularità adeguata a consentire le diverse analisi ed aggregazioni richieste dalle procedure di sfruttamento*" - potrebbe, ad una prima lettura, sembrare scontato.

Sezione VI – L'esternalizzazione di sistemi e servizi ICT

2. Accordi con i fornitori e altri requisiti

Pag. 59: <<*periodica produzione e messa a disposizione dell'intermediario delle opportune copie di backup di dati (database, transazioni, log applicativi e di sistema)*>>

Sul punto segnala l'opportunità, al fine di rafforzare la sicurezza dei sistemi del committente, di sostituire il termine "*copie di back-up dei dati*" con "*copie di backup del proprio patrimonio informatico*".

3. Indicazioni particolari

Viene introdotta la tematica del "cloud computing" la cui definizione risulta, nel suo utilizzo corrente, estremamente generica e comprendente differenti accezioni di servizi e architetture.

La descrizione fornita nelle norme ("*fruizione delle risorse informatiche nella forma di servizi accessibili via rete e configurabili in modo flessibile*") rappresenta senza alcun dubbio un passo ulteriore nel circoscrivere la particolare tematica e, tuttavia, risulta ancora non sufficientemente selettiva, potendo ricomprendere anche servizi già forniti nel passato, ma che difficilmente si assocerebbero oggi al termine "cloud computing", come ad es. l'utilizzo di sistemi informativi di base sviluppati e forniti da centri servizi specializzati su reti non pubbliche.

Risulterebbe quindi utile introdurre una definizione di "cloud computing" che caratterizzi meglio, almeno per le finalità della normativa in consultazione, le condizioni costitutive del cloud da assoggettare alle prescrizioni, facendo ad esempio riferimento a:

- specifiche tecnologie e architetture ricadenti nella definizione (ad es. l'utilizzo di internet combinato ad una allocazione dinamica – e non programmabile - delle risorse decentrata su diversi centri di elaborazione);
- ambito dei servizi a tal fine interessati dal Provvedimento (ad es. servizi finalizzati all'erogazione ed alla gestione di servizi di pagamento, con esclusione di servizi di community verso la clientela (forum, blog, ecc.).

Allegato B – Misure in materia di servizi telematici per la clientela

La tematica delle misure in materia di servizi telematici per la clientela risulta già trattata nel Provvedimento di Attuazione del Titolo II del Decreto legislativo n. 11 del 27 gennaio 2010 (PSD)

(specificatamente nell'Allegato "Tipologie di strumenti di più elevata qualità sotto il profilo della sicurezza") e nelle "Recommendations for the Security of Internet Payments" (ECB).

In particolare, alcune delle misure qui richieste, sono individuate dal Provv. di attuazione della PSD come "Requisiti degli strumenti "a maggior sicurezza"", lasciando ai responsabili dei sistemi il diritto/dovere di implementare soluzioni in base a valutazioni di rischio.

Al fine di facilitare l'implementazione delle misure richieste, risulterebbe utile procedere ad una omogeneizzazione organica dei requisiti o, in questa sede, limitarsi ad un richiamo alle normative esistenti (scelta adottata, ad esempio, nel Provv di attuazione PSD: "*i prestatori di servizi di pagamento si attengono ai requisiti di sicurezza definiti nell'ambito dell'Eurosistema con riferimento agli strumenti di pagamento offerti alla clientela finale*").

1. Verifica dell'autenticità del sito web e cifratura del canale di comunicazione

Pag. 62: << *Al fine di attenuare i rischi di frodi e abusi commessi attraverso falsi siti web che replicano l'apparenza di siti di intermediari, devono essere resi disponibili ai clienti appropriati strumenti per riconoscere i siti web utilizzati per l'erogazione di servizi telematici e per verificarne l'autenticità (ad es. nomi di dominio che rispecchiano la denominazione dell'intermediario, certificati digitali emessi da una riconosciuta autorità di certificazione a nome dell'intermediario)*>>

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

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

L'utilizzo di specifici fornitori di servizio è poi pratica diffusa in tema di autenticazione delle transazioni internet legate alle Carte di pagamento (fornitori del servizio cosiddetto 3D-Secure). In entrambi i casi, l'utilizzo di fornitori specializzati limita gli impatti economici sul singolo intermediario e può favorire l'implementazioni di sistemi complessivamente più sicuri.

Pag. 62: << *Il canale di comunicazione telematica tra intermediario e cliente deve essere cifrato – mediante robuste soluzioni tecnologiche – senza soluzione di continuità (modalità end-to-end), ogni qualvolta siano scambiati dati personali o comunque riservati, ovvero si acceda a funzioni dispositive*>>

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

2. Procedura di autenticazione del cliente

Pag. 62: << *Per minimizzare i rischi di furto di identità, l'accesso del cliente a funzionalità di consultazione o l'attivazione di operazioni su rapporti in essere con l'intermediario devono essere soggetti ad una idonea procedura di autenticazione; almeno con riferimento all'operatività a carattere dispositivo, tale procedura deve fare ricorso a sistemi di autenticazione a più fattori tra loro indipendenti ("autenticazione forte").*>>

Sul punto, si segnala l'inopportunità di una applicazione estensiva delle metodologie di "autenticazione forte" a contesti che, come quelli legati all'utilizzo delle carte di pagamento su internet, prevedono standard di sicurezza fra soggetti diversi senza l'utilizzo di tali modalità (cfr. "3Dsecure").

3. Autorizzazione e monitoraggio delle transazioni di pagamento

Pag. 62: <<*L'intermediario deve disporre di procedure per assicurare che ogni transazione di pagamento sia eseguita solo previa autorizzazione da parte dell'utente*. >>

Risulterebbe utile indicare le relazioni tra il requisito e:

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

Capitolo 9 – Disposizioni in materia di continuità operativa

Il testo in consultazione aggiorna tra le altre cose le "Linee guida per le infrastrutture qualificate del sistema dei pagamenti" emanate a novembre del 2004 ed assume quindi un particolare rilievo.

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

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

In tale prospettiva, si segnalano di seguito i principali passi della precedente normativa:

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

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