DISPOSIZIONI DI VIGILANZA PRUDENZIALE PER LE BANCHE

SISTEMA DEI CONTROLLI INTERNI, SISTEMA INFORMATIVO E CONTINUITA' OPERATIVA

RESOCONTO DELLA CONSULTAZIONE

Rispondenti	– **Assifact** – **Associazione Bancaria Italiana (ABI)** – **Associazione dei Componenti degli Organismi di Vigilanza (AODV)** – **Associazione Italiana Banche Estere (AIBE)** – **Associazione Italiana Compliance (AICOM)** – **Associazione Italiana Information System Auditors (AIEA-ISACA)** – **Associazione Italiana Internal Audit (AIIA)**	– **Associazione Italiana Responsabili Antiriciclaggio (AIRA)** – **Associazione Italiana Revisori Contabili (Assirevi)** – **Associazione Nazionale Direttori Amministrativi e Finanziari (ANDAF)** – **Associazione Nazionale fra le Banche Popolari (ANBP)** – **Assosim** – **Credito Cooperativo Veneto (FVBCC)** – **Federcasse**	– **Banca Nazionale del Lavoro (BNL)** – **Banca popolare di Marostica** – **BCC Carugate** – **Deutsche Bank (DB)** – **ICCREA** – **UBI** – **Unicredit** – **Veneto Banca**	– **Alezio.Net Consulting** – **Cabel Holding S.p.A.** – **Carminati** – **Cedacri-SEC** - ISIDE – **Eddystone S.r.l.** – **Ossola** – **Prospero** – **Orrick** – **Spagnuolo** – **Sottoriva** – **Studio legale Cardia** – **Vasiledi**

Legenda	CRO	Responsabile del RM – *Chief Risk Officer*
	IA	Funzione di revisione interna – *Internal audit*
	OdV	Organismo di Vigilanza ex d.lgs. 231/2001
	OFC	Organo con funzione di controllo

	OFG	Organo con funzione di gestione
	OFSS	Organo con funzione di supervisione strategica
	RAF	*Risk appetite framework*
	RM	Funzione di controllo dei rischi – *Risk management*
	SCI	Sistema dei controlli interni

CAPITOLO 7 Il sistema dei controlli interni

A. Risposte ai BOX

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

La tolleranza al rischio (*risk tolerance*) e l'appetito per il rischio (*risk appetite*) sono entrambi utilizzati per descrivere sia il livello assoluto di rischio che una banca è a priori disposta ad assumere, sia i limiti effettivi che essa pone nell'ambito di tale livello massimo.

Al fine di valutare l'opportunità di individuare parametri utilizzabili per determinare il livello di rischio assumibile, si sollecita l'indicazione delle variabili quantitative e qualitative correntemente utilizzate o in via di sviluppo per addivenire a tale determinazione.

Commenti e proposte

1. Definizione precisa dei concetti di appetito e tolleranza al rischio

Viene posta l'esigenza di fare chiarezza sulla definizione dei termini utilizzati: in particolare, come emerge anche dalla letteratura esistente in materia, i concetti di "appetito" e di "tolleranza" al rischio non sempre hanno un significato univoco né essi sono sempre utilizzati come sinonimi.

2. Indicatori di appetito/tolleranza al rischio

Sono stati proposti due approcci per la definizione di "appetito" e "tolleranza" al rischio:

- approccio analitico: definizione di un *panel* di indicatori (quantitativi e qualitativi) di appetito/tolleranza al rischio distinti per le diverse tipologie di rischio;
- approccio sintetico: creazione di un unico indice di rischio come combinazione di indicatori di rischio di natura diversa, opportunamente normalizzati e ponderati. Tale indice presenta lo svantaggio di fornire un parametro difficilmente interpretabile, in quanto costituito da indicatori per i singoli segmenti di rischio non necessariamente omogenei.

In entrambi i casi, gli indicatori quantitativi indicati includono misure di capitale economico/capitale a rischio, requisiti patrimoniali, misure non ponderate (elementi di stato patrimoniale). Gli indicatori qualitativi individuati sono invece il rating obiettivo della banca e *statement* sulle tipologie o sui fattori di rischio che non si vogliono assumere o che si vogliono contenere.

In coerenza con il principio di proporzionalità, viene inoltre proposto, per le banche di minore dimensione e complessità operativa (es. terza classe ICAAP o quarta macro-categoria SREP), l'individuazione di parametri più comunemente utilizzati nelle prassi aziendali (essenzialmente *core tier 1 ratio* e *total capital ra-*

tio ovvero indicatori analoghi che tengano conto anche dei rischi di secondo pilastro).
È stata sottolineata l'importanza di definire indicatori quali-quantitativi *business-specific* nonché l'inopportunità di utilizzare indicatori quantitativi per i rischi di non conformità, legali e reputazionali.
Partendo dall'osservazione che le prassi aziendali differiscono significativamente, è stato suggerito di definire un "contenuto minimale" per il RAF che preveda obiettivi e limiti almeno in termini di assorbimento di capitale (per i rischi quantificabili) e liquidità, nonché indicazioni in grado di cogliere l'esposizione ai rischi legali, reputazionali, di *compliance*.
Sono stati proposti elementi qualitativi per i rischi difficilmente misurabili (in particolare, di reputazione e di non conformità) o per gli *statement* generali sulle politiche di rischio e indicatori quantitativi per gli altri rischi (indicatori qualitativi: prezzo delle azioni, rating assegnato all'azienda e al suo marchio, capacità di attrarre le migliori professionalità; indicatori quantitativi: indicatori di *performance*, di rischio, di controllo nonché soglie di allerta e sanzioni).

Valutazioni

1. Definizione precisa dei concetti di appetito e tolleranza al rischio

L'esigenza delle banche di fare chiarezza sul contenuto dei termini utilizzati in tema di RAF è condivisibile, dato che esistono definizioni variegate sia nelle prassi aziendali, sia nella letteratura accademica, sia nei testi (raccomandazioni, *guideline*, normative) emanati dai vari *standard setter* nazionali e internazionali. Di recente, anche il Financial Stability Board (FSB) ha sottolineato la necessità che le autorità forniscano *guideline* in materia di RAF, in particolare con riferimento alla tassonomia dei concetti utilizzati (cfr. FSB, "*Thematic Review on Risk Governance - Peer Review Report*", 12 febbraio 2013).

Le disposizioni sono state modificate introducendo le seguenti definizioni:

- ***risk appetite framework* - "RAF"** (sistema degli obiettivi di rischio): il quadro di riferimento che definisce - in coerenza con il massimo rischio assumibile, il *business model* e il piano strategico - la propensione al rischio, le soglie di tolleranza, i limiti di rischio, i processi di riferimento necessari per definirli e attuarli;
- ***risk capacity*** (massimo rischio assumibile): il livello massimo di rischio che una banca è tecnicamente in grado di assumere senza violare i requisiti regolamentari o gli altri vincoli imposti dagli azionisti o dall'autorità di vigilanza;
- ***risk appetite*** (obiettivo di rischio o propensione al rischio): il livello di rischio (complessivo e per tipologia) che la banca intende assumere per il perseguimento dei suoi obiettivi strategici;
- ***risk tolerance*** (soglia di tolleranza): la devianza massima dal *risk appetite* consentita; la soglia di tolleranza è fissata in modo da assicurare in ogni caso alla banca margini sufficienti per operare, anche in condizioni di stress, entro il massimo rischio assumibile;
- ***risk profile*** (rischio effettivo): rischio effettivamente assunto, misurato in un determinato momento di tempo;
- ***risk limits*** (limiti di rischio): l'articolazione degli obiettivi di rischio in limiti operativi, definiti, in linea con il principio di proporzionalità, per tipologie di rischio,

unità e o linee di *business*, linee di prodotto, tipologie di clienti.

2. Indicatori di appetito/tolleranza al rischio

Un RAF efficace presuppone necessariamente l'utilizzo di metriche quantitative ma anche di indicazioni qualitative per la definizione del *risk appetite* (e quindi, a scalare, degli altri elementi che compongono il sistema); in assenza di parametri (quantitativi e qualitativi) che definiscono i rischi, il RAF perde di significato e, soprattutto, se ne pregiudica un effettivo utilizzo gestionale.

Ciò premesso, va però tenuto conto che le prassi aziendali (anche a livello internazionale) sono molto eterogenee: esse scontano le notevoli differenze esistenti nei sistemi di definizione e misurazione dei rischi, diretta conseguenza anche delle caratteristiche dimensionali e operative degli intermediari.

Pertanto, sarebbe inopportuno fornire puntuali indicazioni sui parametri da utilizzare: ne deriverebbero vincoli troppo onerosi, in caso di definizioni ampie e sofisticate, ovvero rischi di appiattimento, in caso di definizioni più standard e semplificate.

Si ritiene invece di ausilio l'enunciazione di alcuni principi definiti cui informare la struttura del RAF:

1. contenuto minimale: il RAF deve prevedere obiettivi, soglie di tolleranza (ove definite) e limiti di rischio in termini di:
   a) misure espressive del capitale a rischio o capitale economico (VaR, *expected shortfall*, ecc.);
   b) adeguatezza patrimoniale;
   c) liquidità.

   Inoltre, deve fornire indicazioni in merito ai principali rischi difficilmente quantificabili (di reputazione, di *compliance*, ecc.).
2. utilizzo di parametri quantitativi e qualitativi: per i rischi quantificabili, la declinazione di propensione al rischio, soglie di tolleranza, limiti di rischio deve avvenire attraverso opportuni parametri quantitativi; per i rischi difficilmente quantificabili e/o per eventuali *statement* generali sulle politiche di rischio che la banca intende seguire, va fatto ricorso a indicazioni di tipo qualitativo in grado di orientare la definizione e l'aggiornamento di processi e sistemi di controllo;
3. principio di proporzionalità: i parametri quantitativi e qualitativi utilizzati nella definizione del RAF devono essere coerenti con quelli utilizzati in sede di pianificazione patrimoniale (ICAAP) e strategica.

3. Ruolo degli organi aziendali e delle funzioni di controllo

Alla definizione e al monitoraggio del RAF concorrono – ciascuno secondo il rispettivo ambito di responsabilità – sia gli organi aziendali sia le funzioni di controllo. In particolare:

- ***OFSS***: definisce e approva gli obiettivi di rischio, la soglia di tolleranza (ove identificata) e le politiche di governo dei rischi; assicura che l'attuazione del RAF sia coerente con gli obiettivi di rischio e la soglia di tolleranza e ne valuta periodicamente l'adeguatezza e l'efficacia; assicura la coerenza complessiva del RAF con il piano strategico, l'ICAAP, i budget e il sistema dei controlli nonché la compatibilità tra il rischio effettivo e gli obiettivi di rischio;
- ***OFG***: cura l'attuazione del RAF e individua le azioni gestionali da intraprendere al raggiungimento della soglia di tolleranza (se definita); definisce e cura

l'attuazione del processo di gestione dei rischi e, in tale ambito, stabilisce i limiti operativi all'assunzione delle varie tipologie di rischio; assicura la coerenza dei processi aziendali (quali quelli di gestione dei rischi, di approvazione di nuovi prodotti e servizi, l'avvio di nuove attività e l'inserimento in nuovi mercati) con la propensione al rischio; definisce i flussi informativi interni volti ad assicurare agli organi aziendali e alle funzioni di controllo la piena conoscenza e governabilità dei fattori di rischio e la verifica del rispetto del RAF;

- ***OFC***: vigila sulla completezza, adeguatezza, funzionalità e affidabilità del sistema dei controlli interni e del RAF;
- ***RM***: è coinvolta nella definizione del RAF, delle politiche di governo dei rischi e delle varie fasi che costituiscono il processo di gestione dei rischi nonché nella fissazione dei limiti operativi all'assunzione delle varie tipologie di rischio. In tale ambito, ha, tra l'altro, il compito di proporre i parametri quantitativi e qualitativi necessari per la definizione del RAF, che fanno riferimento anche a scenari di *stress* e, in caso di modifiche del contesto operativo interno ed esterno della banca, l'adeguamento di tali parametri; dà pareri preventivi sulla coerenza con il RAF delle operazioni di maggiore rilievo eventualmente acquisendo, in funzione della natura dell'operazione, il parere di altre funzioni coinvolte nel processo di gestione dei rischi;
- ***IA***: valuta l'efficacia del processo di definizione del RAF, la coerenza interna dello schema complessivo e la conformità dell'operatività aziendale al RAF e, in caso di strutture finanziarie particolarmente complesse, la conformità di queste alle strategie approvate dagli organi aziendali.

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

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

Commenti e proposte

È stato chiesto di mantenere l'impostazione del documento che attribuisce all'OFSS il compito di definire i criteri per l'identificazione delle operazioni di maggior rilievo.

È stato suggerito di non rendere il parere ridondante rispetto a quello formulato dai soggetti che propongono l'assunzione del rischio. Il parere dovrebbe concorrere ad arricchire la prospettiva di giudizio promuovendo una visione olistica e non focalizzandosi su un singolo rischio. Esso potrebbe riguardare una valutazione circa la potenziale redditività dell'operazione ma non dovrebbe riguardare aspetti di competenza di altre funzioni.

Tra i criteri proposti per identificare le operazioni di maggior rilevo sono stati proposti:

- l'apporto marginale che la potenziale operazione potrebbe produrre in termini di assorbimento del livello di *risk tolerance* prescelto dall'OFSS;
- la percentuale di assorbimento del Capitale Interno (singolo rischio) e del Capitale Interno Complessivo che l'operazione di particolare rilievo potrebbe determinare;

Inoltre si potrebbero considerare operazioni di maggior rilievo quelle:

- poste in essere con parti correlate e soggetti collegati come definite dal Titolo V, Capitolo 5, della Circolare 263 e che al contempo superino una certa soglia di importo
- che assumono carattere di straordinarietà, quali acquisizioni di un ramo d'azienda, o di aziende, piuttosto che acquisizioni/cessioni di partecipazioni di controllo, ecc.

È stato suggerito di identificare le operazioni di maggior rilievo con quelle che modificano l'operatività della banca quali:

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

Sono stati suggeriti i seguenti ulteriori criteri per individuare le operazioni di maggior rilievo:

- controparte/i coinvolta/e. Le operazioni con controparti aventi sede in una giurisdizione "non trasparente", ovvero la cui struttura societaria presenta elementi di "opacità" e/o di complessità, ovvero che possano dar luogo a situazioni di conflitto di interesse oppure appartengono a specifiche categorie sensibili (aziende della PA);
- tipologia dell'operazione. Le operazioni che, pur nell'ambito della operatività della banca, implichino delle specifiche deroghe a significativi standard operativi e contrattuali (ad es., operazioni di investimento effettuate attraverso il ricorso a SPV o altre strutture societarie complesse);
- coerenza con gli indirizzi strategici della banca.
- operazioni non ricorrenti o abituali, significative per dimensioni e generalmente complesse: scadenza insolitamente lontana, dimensione eccezionale, complesse in termini di remunerazione, del sistema delle garanzie e più generalmente della strutturazione dell'operazione stessa (algoritmi o strutture di pricing complessi o caratteristiche che sollevino nuovi problemi legali, di *compliance* o regolamentari).

Valutazioni

Si conferma l'impostazione del documento di consultazione di rimettere all'OFSS la competenza a individuare i criteri con cui identificare le operazioni di maggior rilievo.

Si precisa tuttavia che tali operazioni non devono ricadere nella competenza diretta degli organi aziendali, nel qual caso il parere del RM sarebbe consultivo.

I criteri individuati per identificare le operazioni di maggiore rilievo devono essere coerenti con il RAF e idonei a censire le operazioni in caso vi siano potenziali conflitti di interesse.

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

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

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

Commenti e proposte

Sono stati suggeriti i seguenti criteri per declinare il principio di proporzionalità con riferimento all'accorpamento/esternalizzazione delle funzioni aziendali di controllo:

- quotazione dell'intermediario;
- tipologia di attività svolta;
- fatturato;
- dimensione del patrimonio gestito;
- controvalore delle negoziazioni effettuate;
- utilizzo di sistemi interni di misurazione dei rischi;
- macro-categoria SREP di appartenenza.
- criteri individuati dall'ESMA per decidere quali misure siano adeguate per garantire l'efficacia della funzione di controllo della conformità alla luce delle circostanze particolari dell'impresa;
- macrocategorie SREP;
- dimensioni (il fatturato, il numero dei dipendenti, il numero dei canali di vendita, il numero di dipendenze) e complessità operativa (numero di *business line* su cui si è attivi, dotazione di risorse umane e tecnologiche, operatività transfrontaliera);
- metrica utilizzata per individuare le *domestic SIFIs*.

Valutazioni

Le disposizioni sono state modificate per meglio chiarire e differenziare la disciplina i) dell'esternalizzazione all'esterno del gruppo di appartenenza (che comporta la dipendenza per lo svolgimento di una determinata attività da un soggetto esterno alla banca o al proprio gruppo), da quella ii) dell'esternalizzazione presso la capogruppo o altra componente del gruppo, che costituisce una riallocazione organizzativa dei compiti all'interno di un gruppo sottoposto a direzione e coordinamento unitari.

i) Esternalizzazione all'esterno del gruppo

Il principio di proporzionalità è stato declinato in termini puntali con riferimento all'esternalizzazione delle sole funzioni aziendali di controllo e non anche con riguardo alle altre funzioni operative importanti. In particolare:

- è stato precisato che l'esternalizzazione delle funzioni aziendali di controllo a soggetti terzi dotati di requisiti idonei in termini di professionalità e indipendenza è ammessa, di norma, per le sole banche classificate, a fini SREP, nella macro-categoria 4;
- è stato precisato che la nomina dei referenti interni delle funzioni aziendali di controllo esternalizzate deve avvenire con le stesse modalità e garanzie previste per la nomina dei responsabili di funzioni aziendali di controllo, in caso di non esternalizzazione di quest'ultime;
- sono state inserite prescrizioni più puntuali, al fine di evitare l'insorgere di conflitti di interesse, in tema di indipendenza del soggetto terzo;
- sempre al fine di garantire l'indipendenza, inoltre, è stato prescritto che il soggetto terzo che svolge i controlli in *outsourcing*:
    - non cumuli le funzioni di controllo di II e III livello per un medesimo soggetto che esternalizza;
    - non svolga già la funzione di revisione legale dei conti, in analogia con quanto già disciplinato dal d.lgs. 39/2010 ([1]);
- è stato precisato il termine entro il quale comunicare all'autorità l'intenzione di esternalizzare.

ii) Esternalizzazione presso la capogruppo o altra componente del gruppo:

L'accentramento delle funzioni aziendali di controllo presso la capogruppo di competenze viene regolato in modo autonomo dall'esternalizzazione al di fuori del gruppo.

In generale, l'accentramento di dette funzioni non elimina l'obbligo posto in capo agli organi di vertice delle singole controllate di tutelare l'interesse della società da essi amministrata, dei depositanti di questa e degli eventuali azionisti di minoranza. Essi, dunque, rimangono responsabili del buon funzionamento del sistema dei controlli interni della banca.

Ciò posto, l'esternalizzazione infragruppo è consentita per tutte le banche indipendentemente dalle loro dimensioni o complessità operativa; sono stati, inoltre, dettati alcuni criteri in base ai quali le banche effettuano le scelte connesse all'esternalizzazione all'interno del gruppo.

[1] Art. 17 c. 1, d.lgs. 39/20120 in tema di revisione legale dei conti, attuazione della direttiva 2006/43/CE: "… *le società di revisione legale […] non possono fornire alcuno dei seguenti servizi all'ente di interesse pubblico* (tra cui le banche) *che ha conferito l'incarico di revisione: e) gestione esterna dei servizi di controllo interno…;*"

B. Osservazioni alle disposizioni

CAPITOLO 7 Il sistema dei controlli interni

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
Sezione I (Disposizioni preliminari e principi di carattere generale), par. 1 (Premessa)	**Inquadramento della funzione antiriciclaggio** È stato chiesto di chiarire se il Capitolo, rappresentando una cornice generale del sistema dei controlli, si debba applicare anche alla funzione antiriciclaggio almeno nelle sue parti generali e non diversamente disciplinate (ad es., la richiesta di invio della relazione annuale) o se questa rimanga regolata esclusivamente dal provvedimento specifico del marzo 2011, anche qualora i compiti antiriciclaggio siano stati assegnati alla *compliance* o al *risk management*.	Chiarimento	Le presenti disposizioni si applicano anche alla funzione antiriciclaggio per le parti non diversamente disciplinate dal provvedimento del marzo 2011.
	Definizioni È stato chiesto di utilizzare la locuzione "sistema di controllo interno", al singolare, invece di "sistema di controlli interni".	No	L'espressione utilizzata nel documento di consultazione appare maggiormente in linea con quella adottata dall'art. 53, comma 1, lett. d) del TUB ("controlli interni").
	È stato chiesto di aggiungere nella locuzione di "Sistema dei controlli interni" il riferimento alla "gestione dei rischi".	No	La gestione dei rischi è un processo trasversale che coinvolge sia funzioni operative che di controllo. Pertanto, le disposizioni, riguardando il sistema dei controlli interni, non esauriscono tutti gli aspetti legati alla gestione dei rischi.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
Sezione I (Disposizioni preliminari e principi di carattere generale), par. 3 (Definizioni)	È stato chiesto di introdurre la definizione: "e) "Funzione": insieme di compiti e attività assegnate all'interno dell'azienda allo scopo di assicurarne l'esecuzione. Con tale termine non si intende fare riferimento a specifiche strutture organizzative, esistenti o da costituire".	In parte	Si condivide l'esigenza di inserire una definizione di "funzione". Si fa presente che la funzione può anche coincidere con una specifica struttura organizzativa dell'azienda quando i compiti, le attività e le responsabilità della funzione sono tali da richiedere l'istituzione di una specifica struttura.
	È stato chiesto di modificare la definizione di processo di gestione dei rischi specificando il contenuto del termine "risorse" che, avendo una portata di carattere generale, potrebbe rendere meno efficace il valore stesso della definizione fornita. Si potrebbe dunque fare riferimento a "*l'insieme delle regole, delle procedure, della strumentazione (anche informatica), delle attività di controllo e delle risorse umane volte a identificare, misurare o valutare, monitorare, attenuare e comunicare ai livelli appropriati i rischi, come specificato nel par. 5*".	Sì	Testo modificato.
	È stato chiesto di menzionare anche la funzione antiriciclaggio.	Sì	Testo modificato.
	È stato sottolineato che nel Documento di consultazione si riscontrano delle indicazioni (ad es., "funzioni aziendali e societarie di controllo") che non appaiono ricomprese nel perimetro delle "Definizioni". Si suggerisce, pertanto, al fine di evitare fraintendimenti, di allineare tutte le suddette indicazioni al perimetro delle "Definizioni".	Si	Testo modificato.
	Con riferimento alla nozione di "funzioni aziendali di controllo", è stato rilevato un disallineamento con il Do-	Chiarimento	Ferma restando l'esistenza di funzioni di staff che concorrono alla "*second line of defence*", le di-

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	cumento del Comitato di Basilea "*The internal audit function in banks*", principio 13, laddove include nella "*second line of defence*" anche le funzioni di *human resources, technology, legal, finance, operations*, oltre al *risk management* e alla *compliance*.		sposizioni di vigilanza – coerentemente con i principi internazionali – regolano in modo specifico il RM e la *compliance* in quanto sono le funzioni, nell'ambito dei controlli di secondo livello, preposte alla gestione e al monitoraggio dei rischi tipici dell'attività bancaria e di intermediazione in generale (che possono emergere nell'ambito delle funzioni sia di *business*, sia di staff, come nel caso del rischio operativo).
Sezione I (Disposizioni preliminari e principi di carattere generale), par. 6 (Principi generali)	**Aderenza ai principi del sistema dei controlli interni** Con riferimento all'ultimo capoverso "*Le banche verificano regolarmente, con frequenza almeno annuale, il grado di aderenza ai requisiti del sistema dei controlli interni e dell'organizzazione e adottano le misure adeguate per rimediare a eventuali carenze*" è stato chiesto di chiarire: - se sia sufficiente una delibera che valuti le risultanze delle relazioni delle funzioni di controllo corredata delle relative considerazioni dell'OFSS; - se la valutazione debba essere svolta dall'OFSS sentito l'OFC.	Chiarimento	La delibera dell'OFSS che valuti le risultanze delle relazioni delle funzioni di controllo corredata delle relative considerazioni dello stesso organo, sentito anche l'OFC, è l'attività di verifica minimale che deve essere svolta dalle banche. Ci si attende infatti che l'attività di verifica possa avere frequenza maggiore ed essere innescata da flussi informativi diversi dalle relazioni delle funzioni di controllo: in generale, qualsiasi evento astrattamente idoneo a evidenziare carenze nel sistema dei controlli interni va portato a conoscenza degli organi aziendali, che devono verificare la gravità della carenza e porre in essere i rimedi necessari a rimuoverla.
	Ambito della *compliance* e dell'IA È stato chiesto di confermare che gli obiettivi dei controlli di *compliance* riguardino la conformità alle norme esterne dell'operatività aziendale per evitare sovrapposizioni con la verifica del rispetto della regolamentazione interna attribuita alla funzione di revisione interna.	Chiarimento	L'ambito dei controlli della funzione di *compliance* è definito nella Sez. III, par. 3.2; essi sono riferiti alle norme esterne e di autoregolamentazione. L'ambito del controllo della funzione di *internal audit* comprende anche la verifica del rispetto della regolamentazione. Ciò, tuttavia, non determina una sovrapposizione con l'attività della

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
			compliance, in quanto l'IA agisce in un'ottica di controlli di terzo livello (tipicamente *ex post*, non nel continuo), mentre la funzione di conformità alle norme agisce secondo un'ottica di secondo livello.
	Processo di valutazione delle attività aziendali Con riferimento ai processi e alle metodologie di valutazione delle attività aziendali, è stato chiesto di: 1) definire il significato di attività aziendali chiarendo se si tratti di processi operativi o *asset*; 2) chiarire le modalità di integrazione dei processi e delle metodologie di valutazione contabili con quelli di *risk management*; 3) limitare la portata della norma alle sole attività complesse e in assenza di riferimenti di mercato; 4) indicare quali sono gli altri fini, oltre a quelli contabili, per cui tali processi devono essere utilizzati.	Chiarimento	In relazione ai chiarimenti richiesti, si fa presente quanto segue: 1) per attività aziendali si intendono tutti gli elementi che costituiscono l'attivo della banca sia *on-balance*, sia *off-balance*; 2) l'integrazione con il processo di *risk management* è cruciale in quanto questo riguarda in modo trasversale tutta l'operatività aziendale e non è limitato alla sola funzione di controllo dei rischi. L'integrazione deve, ad es., consentire di riconciliare le valutazioni contabili con quelle effettuate a fini di controllo del rischio o a fini operativi/gestionali. I dati e i modelli utilizzati per i vari fini devono essere affidabili e tra loro raccordabili; 3) la norma si applica a tutte le attività; naturalmente, per le attività più complesse, per le quali più frequente è l'utilizzo di modelli e di valutazioni interne, la verifica dell'affidabilità dovrà essere effettuata con particolare cura e attenzione; 4) tra le altre finalità per cui tali processi possono essere utilizzati, si menzionano, a titolo esemplificativo, fini di *risk mana-*

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
			gement o gestionali.
	Responsabilità delle strutture operative È stato chiesto di modificare la responsabilità delle strutture operative prevedendo che le stesse siano responsabili di adottare misure e di mantenere politiche e procedure e non di considerarle responsabili del processo di gestione dei rischi. È stato chiesto di specificare che le funzioni aziendali di controllo hanno l'obietto di "*verificare … la corretta attuazione del processo di gestione dei rischi da parte di tutte le strutture della banca coinvolte*", piuttosto che quello di "*assicurare … la corretta attuazione del processo di gestione dei rischi*".	Chiarimento	La gestione dei rischi è un processo di natura tipicamente trasversale che coinvolge diverse strutture, operative e di controllo, della banca. L'attuale formulazione delle disposizioni sottolinea questa caratteristica, prevedendo che sia le strutture operative, sia le funzioni di controllo, ciascuna per gli aspetti di competenza, concorrano alla corretta attuazione del processo di gestione dei rischi.
	Requisiti di integrazione È stato chiesto di inserire tra i principi generali un'indicazione circa le caratteristiche di integrazione ritenute adeguate: «*Un governo adeguato di tutti i rischi aziendali implica l'adozione di un Processo di gestione dei rischi che sia efficacemente integrato. Sono considerati parametri di integrazione i seguenti elementi: la diffusione di un linguaggio comune nella gestione dei rischi a tutti i livelli della banca; l'adozione di metodi e strumenti di rilevazione e valutazione tra di loro coerenti (ad es.: unica tassonomia dei processi; unica mappa dei rischi); la definizione di modelli di reportistica trasversali alle diverse tipologie di rischio, al fine di favorirne la comprensione e la corretta valutazione; ancora, sotto il profilo della operatività delle funzioni coinvolte nel Processo di gestione del rischio, l'individuazione di momenti formalizzati di coordina-*	Sì	Testo modificato.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	mento ai fini della pianificazione delle rispettive attività sulla base dei rischi in essere; la previsione di flussi informativi su base continuativa tra le diverse funzioni in relazione ai risultati delle attività di controllo di propria pertinenza; la condivisione nella individuazione delle azioni di rimedio».		
	Requisiti di indipendenza dell'unità di valutazione delle attività È stato chiesto di confermare che l'unità responsabile della valutazione degli strumenti finanziari possa essere considerata "indipendente" anche nel caso di collocamento come unità distinta dal *front office*, ma che pur sempre riporta al responsabile della finanza, come spesso avviene per le funzioni di *middle office* delle banche.	Chiarimento	La lettura proposta è coerente con le disposizioni.
	Controlli di linea Con specifico riferimento alla previsione relativa ai controlli di linea, è stato proposto di inserire dopo la frase "*per quanto possibile, essi sono incorporati nelle procedure informatiche*", la frase "*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*".	Sì	Testo modificato.
	Perimetro dell'attività di verifica È stato proposto di estendere a tutte le funzioni di controllo il compito dell'IA di individuare le violazioni delle	Chiarimento	Si ritiene che i compiti attribuiti alle funzioni di controllo (come, ad es., la corretta attuazione del processo di gestione dei rischi, il rispetto dei limiti

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	procedure e della regolamentazione e di accertare le specifiche irregolarità, onde evitare che si crei una sorta di riserva di attività in capo all'IA.		operativi, ecc.) includano anche la verifica del rispetto delle procedure e della regolarità delle attività svolte.
	Natura e ambito dell'attività di IA Con riferimento alle valutazioni dell'IA, è stato chiesto di chiarire se quanto in capo all'IA ("*valutare periodicamente la completezza, la funzionalità e l'adeguatezza, in termini di efficienza e di efficacia, del sistema dei controlli interni* … ") debba essere riferito alle sole parti di sua competenza (in coerenza con quanto, ad es., riportato al penultimo cpv. della Sez. III, par. 2).	Chiarimento	L'IA, in un'ottica di controlli di terzo livello, valuta la completezza, la funzionalità e l'adeguatezza dell'intera struttura organizzativa, incluse le altre componenti del sistema dei controlli interni.
	È stato chiesto di meglio definire il concetto di "completezza" del sistema dei controlli interni, atteso che in generale l'IA può assicurare la completezza limitatamente alle attività svolte nell'ambito del piano annuale di audit.	Chiarimento	La completezza del sistema dei controlli interni va valutata, annualmente, con riferimento alle attività svolte nel piano annuale. In ogni caso, nella valutazione, l'IA tiene conto di tutte le informazioni di cui viene a conoscenza, anche in aggiunta a quelle ottenute in esito alle attività svolte in attuazione del piano.
Sezione I (Disposizioni preliminari e principi di carattere generale)	**Mappatura dei rischi** È stato chiesto: 1) se sia necessaria una mappatura dei rischi formalizzata da rendere disponibile alle varie strutture; 2) il livello di analiticità della mappatura; 3) la possibilità di sviluppare un'unica fase di identificazione dei rischi comune per le funzioni	Chiarimento	Si ritiene necessario che l'OFSS formalizzi e comunichi alle strutture/funzioni interessate la mappatura dei rischi assunti dalla banca, con evidenza dei rischi cui sono esposte le varie unità operative. La fase di identificazione dei rischi può essere, per le parti comuni, unica per tutte le funzioni aziendali di controllo. Il livello di analiticità della mappatura deve essere coerente con il principio di proporzionalità e dunque riflettere le dimensioni e la complessità ope-

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	di controllo di secondo e terzo livello.		rativa della banca.
Sezione II (Il ruolo degli organi aziendali), par. 1 (Premessa)	**Identificazione responsabilità organi aziendali** È stato proposto di introdurre delle indicazioni sintetiche da cui sia possibile evincere le responsabilità dei diversi organi aziendali. E' stato chiesto di prevedere una chiara definizione dei termini "*valutazione*", "*verifica*", "*attuazione*" anche al fine di garantire un corretto esercizio della responsabilità.	In parte	Testo modificato per meglio chiarire la ripartizione delle competenze tra OFSS e OFG.
Sezione II (Il ruolo degli organi aziendali), par. 2 (Organo con funzione di supervisione strategica)	**Pianificazione attività funzioni di controllo e piano audit** È stato evidenziato che il coinvolgimento dell'OFSS dovrebbe qualificarsi più propriamente come "*approvazione*", anziché come "*esame*", "*del programma di attività [omissis] predisposti dalle funzioni aziendali di controllo compreso il piano di audit predisposto dalla funzione di revisione interna*".	In parte	Il testo è stato modificato per chiarire che il programma di attività e il piano audit vanno approvati dall'OFSS, mentre le relazioni annuali sono esaminate dallo stesso organo.
	È stato chiesto di citare, oltre ai piani annuali, anche il piano strategico o pluriennale di audit	Sì	Testo modificato.
	Relazione sui modelli interni È stato osservato che non è stato ripreso l'esplicito riferimento alla Relazione Annuale predisposta dalla funzione di revisione interna con riferimento ai sistemi interni di misurazione dei rischi, prevista dalla disciplina vigente (cfr. Titolo II (requisiti patrimoniali) – parte II (metodologia basata sui rating interni IRB) della Circ.	Chiarimento	Si fa presente che l'informativa che la funzione di revisione interna deve rendere in ordine ai sistemi IRB (cfr. Circolare n. 263, Titolo II, Capitolo 1, Parte II, Sez. III, par. 2.2) dovrà essere resa nella relazione annuale che l'IA trasmette agli organi aziendali secondo quanto previsto nella Sezione III, par. 2 delle disposizioni in materia di sistema dei controlli interni.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	263/2006).		
	Valutazione finale del SCI È stato suggerito di sottolineare con maggiore evidenza a quale organo è attribuita la valutazione finale del sistema dei controlli interni.	Chiarimento	La norma attribuisce la responsabilità ultima di approvare l'architettura e le modalità di funzionamento del sistema dei controlli interni all'OFSS.
	Modelli interni non utilizzati a fini regolamentari È stato chiesto di precisare il contenuto minimo della verifica periodica sul corretto funzionamento dei sistemi interni di misurazione dei rischi non utilizzati a fini regolamentari non essendo ipotizzabile che i sistemi gestionali vengano sottoposti a un processo di convalida analogo al processo previsto per la convalida dei sistemi regolamentari, la cui verifica è estremamente onerosa.	Chiarimento	La norma ha la finalità di assicurare che anche i modelli di misurazione dei rischi usati solo a fini gestionali siano affidabili. Ciò posto, le disposizioni rimettono all'autonomia dell'OFSS, che ne assume la relativa responsabilità, la determinazione delle condizioni per l'approvazione di tali modelli e dei controlli da effettuare per assicurarne il corretto funzionamento.
	Succursali di banche comunitarie Con riferimento alle succursali di banche comunitarie, è stato chiesto quale sia il ruolo del *country manager* e se questi può essere visto al pari dell'OFSS e dell'OFG.	Chiarimento	Le presenti disposizioni si applicano alle succursali di banche comunitarie nei limiti indicati dalla Sezione VIII del documento di consultazione.
	Riparto di competenze tra OFSS e OFG È stato chiesto di ampliare gli ambiti in cui l'OFSS si assicuri che certe attività, processi o strumenti vengano approntati dall'OFG e, parallelamente, diminuire quelli sottoposti alla sua diretta approvazione e che comportano assunzione di responsabilità. È stato chiesto di chiarire meglio i ruoli dell'OFSS e	In parte	Testo modificato. Le materie ricondotte all'approvazione dell'OFSS hanno una rilevanza strategica per la conduzione dell'attività bancaria e pertanto si ritiene necessaria una specifica assunzione di responsabilità da parte del *board*. Tuttavia, il testo è stato modificato per meglio

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	dell'OFG per quanto riguarda la definizione dei compiti e delle responsabilità delle funzioni coinvolte nel processo di gestione dei rischi. Infatti, da un lato, si propone di attribuire all'OFSS l'approvazione delle funzioni aziendali e societarie di controllo, nonché i relativi compiti e responsabilità, mentre, dall'altro, viene attribuito all'OFG il compito di stabilire le responsabilità delle strutture e delle funzioni aziendali coinvolte nel processo di gestione dei rischi. Analogamente è attribuita all'OFSS l'approvazione dei flussi informativi tra le funzioni di controllo e tra queste e gli organi aziendali, mentre l'OFG definisce "*i flussi informativi interni volti ad assicurare agli organi aziendali e alle funzioni aziendali di controllo la piena conoscenza e governabilità dei fattori di rischio*" . Nello stesso senso, è stato richiesto di chiarire il significato di espressioni simili, ma che possono comportare letture differenti ("esamina/valuta", "definisce/approva", "sottopone/propone", ecc.).		precisare i compiti e le relative responsabilità dell'OFSS e dell'OFG.
	Adeguamento alle nuove disposizioni È stato chiesto di chiarire se eventuali politiche, processi o attività già approvati da organi aziendali diversi da quelli indicati nel documento, debbano essere sottoposti nuovamente all'approvazione dell'organo ritenuto competente in base alle indicazioni contenute nelle presenti disposizioni.	Chiarimento	Si ritiene che le politiche e i processi approvati in passato da organi diversi da quelli competenti ai sensi delle nuove disposizioni di vigilanza vadano riesaminati dagli organi competenti.
	Giurisdizioni poco trasparenti È stato chiesto se l'individuazione delle giurisdizioni poco trasparenti possa essere effettuata utilizzando	Chiarimento	L'individuazione di tali giurisdizioni è rimessa all'autonomia delle banche. A tal fine, l'utilizzo di *scoring* definiti da organismi o istituzioni sovranazionali riconosciute attendibili può costituire un

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	scoring definiti da organismi o istituzioni sovranazionali (es: Transparency International).		valido ausilio per individuare le giurisdizioni poco trasparenti. Tuttavia, la banca non deve fare meccanico affidamento su tali valutazioni.
	Identificazione dell'OFG È stato chiesto di chiarire se la qualifica di OFG possa essere attribuita, in funzione delle specifiche mansioni, a differenti organi/soggetti (ad es., comitato esecutivo, amministratore delegato, direttore generale).	Chiarimento	L'individuazione dell'OFG è disciplinata dalle disposizioni di vigilanza in materia di organizzazione e governo societario delle banche del 4 marzo 2008, cui si rimanda.
	Poteri del RM e operazioni di maggior rilievo È stato chiesto di coordinare le disposizioni che disciplinano il potere del RM con riferimento alle operazioni di maggior rilievo (par. 2, secondo alinea, lett. c), con quelle che disciplinano in generale le funzioni di controllo (par. 2, terzo alinea, lett. a) e con quelle relative ai compiti dell'OFG in materia di operazioni di maggior rilievo (par. 3, primo alinea, lett. d).	Sì	Testo modificato.
	OFSS e assetti organizzativi delle funzioni di controllo È stato osservato che la norma relativa alla costituzione delle funzioni aziendali di controllo è ampia e potrebbe portare l'OFSS a occuparsi sin nella loro granularità degli assetti organizzativi delle funzioni aziendali di controllo. È stato quindi proposto di chiarire che la competenza deliberativa in capo all'OFSS riguarda esclusivamente le strutture che fanno capo ai responsabili delle funzioni di controllo e non anche le singole unità di cui tali strutture si compongono.	Chiarimento	Si condivide l'osservazione. La norma prevede che l'OFSS debba approvare la costituzione delle funzioni aziendali di controllo, le modalità di coordinamento e collaborazione tra le funzioni e i relativi flussi informativi. Non viene invece richiesto che l'OFSS approvi l'articolazione interna delle varie funzioni di controllo (ossia l'organizzazione delle eventuali unità di cui queste si compongono) che può essere rimessa all'OFG.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	Continuità operativa È stato chiesto, in analogia a quanto previsto nelle disposizioni emanate nel luglio 2004, di chiarire i compiti degli organi aziendali con riferimento alla *business continuity*.	Sì	È stato modificato il Capitolo 9 in materia di continuità operativa.
	È stato chiesto, al fine di mantenere una definizione unitaria dei compiti degli organi aziendali di aggiungere in tale sede il compito di approvare il piano di continuità operativa.	Sì	È stato modificato il Capitolo 9 in materia di continuità operativa.
Sezione II (Il ruolo degli organi aziendali), par. 3 (Organo con funzione di gestione)	**Processo di approvazione dei nuovi prodotti** Nell'ambito della definizione del processo diretto alla distribuzione di nuovi prodotti e con particolare riferimento alla distribuzione dei nuovi prodotti di investimento, è stato chiesto di rendere coerente tale previsione con la regolamentazione Consob in materia di obblighi di valutazione di adeguatezza a carico degli intermediari.	Chiarimento	Il processo di approvazione di nuovi prodotti/servizi/attività ha un ambito applicativo generale. L'obiettivo è, infatti, quello di assicurare che la banca valuti, prima di avviare una nuova operatività, tutti i rischi derivanti da nuovi prodotti/servizi/attività, non solo quelli derivanti dalla violazione della normativa di tutela della clientela (ad es., obblighi di valutazione dell'adeguatezza / appropriatezza previsti dalla disciplina attuativa della MiFID). Sotto quest'ultimo profilo, la banca, nella definizione del processo, terrà conto anche dell'eventuale disciplina specifica del nuovo prodotto o servizio.
	Gestione integrata dei rischi Si chiede di meglio precisare il significato della locuzione "gestione integrata" in relazione con il "principio di proporzionalità". Ad es., si chiede di chiarire se l'approccio *building block*, utilizzato per la determina-	Chiarimento	La gestione integrata dei rischi attiene in primo luogo a profili di natura gestionale – organizzativa: nel momento in cui la banca assume, in linea con i propri obiettivi, un determinato rischio, questa deve valutare gli effetti che tale assunzione di rischio ha sugli altri rischi assunti nonché, ove

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	zione del capitale interno complessivo e che esclude le correlazioni tra i rischi, può essere coerente con la gestione integrata dei rischi richiesta.		necessario, rafforzare i presidi organizzativi e patrimoniali. Quanto agli aspetti relativi alla quantificazione del capitale, nel processo di aggregazione dei rischi le banche devono identificare e valutare gli effetti delle concentrazioni che possono emergere dall'interazione tra i diversi rischi, soprattutto in condizioni di stress. In applicazione del principio di proporzionalità, le banche di minore dimensione e complessità possono limitarsi a sommare il capitale interno calcolato a fronte dei singoli rischi e valutare le interazioni tra i rischi adottando un approccio qualitativo e semplificato.
	Ruolo del direttore generale Si chiede di confermare la possibilità, con riferimento agli intermediari creditizi che adottino il sistema tradizionale, di incentrare taluni dei compiti definiti in merito alla strutturazione e al funzionamento del sistema dei controlli interni per l'Organo con Funzione di Gestione sulla Direzione Generale, eventualmente dandone una declinazione puntuale e circoscritta. A tale riguardo potrebbe risultare, ad es., utile l'introduzione di una prescrizione quale la seguente: "*il direttore generale può essere destinatario di deleghe da parte dell'organo con funzione di supervisione strategica in materia di strutturazione e funzionamento del sistema dei controlli interni*".	Chiarimento	L'individuazione dell'OFG e i rapporti con il direttore generale sono disciplinati dalle disposizioni di vigilanza in materia di organizzazione e governo societario delle banche del 4 marzo 2008, cui si rimanda.
	Formalizzazione delle responsabilità delle funzioni	Sì	Testo modificato.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	di controllo È stato chiesto di inserire un obbligo di formalizzazione e di portare a conoscenza di tutte le strutture le responsabilità assegnate alle varie funzioni aziendali.		
	Mezzi e poteri delle funzioni di controllo È stato chiesto di prevedere che l'OFG assicuri ai soggetti cui sono affidate responsabilità i necessari mezzi e poteri.	Chiarimento	Tale principio è presente esplicitamente nelle disposizioni con riferimento alle funzioni aziendali di controllo. In particolare, si prevede che tali funzioni devono essere dotate, tra l'altro, delle risorse necessarie a svolgere i compiti loro assegnati (cfr. Sez. III, par. 1).
	È stato chiesto di chiarire se la nuova normativa sul sistema dei controlli intenda suggerire soluzioni organizzative specifiche rispetto alla misurazione e al monitoraggio del rischio di modello, posto che essa non intende intervenire sulla disciplina dei requisiti patrimoniali di primo pilastro né su quella del processo di controllo prudenziale (secondo pilastro). In particolare, la valutazione e il monitoraggio del rischio modello sono attualmente inclusi nell'ambito della disciplina sul trattamento dei singoli profili di rischio di primo pilastro. La valutazione complessiva del rischio è poi funzionale alla determinazione del *capital cushion* nell'ambito della disciplina sul processo di controllo prudenziale.	Chiarimento	Tenuto conto della rilevanza del rischio di modello, le disposizioni sui controlli interni richiedono agli organi aziendali piena consapevolezza di tale rischio e l'approntamento di adeguati presidi organizzativi per attenuarlo.
	Ammissibilità dell'OFG monocratico È stato chiesto di chiarire se l'OFG possa essere un organo monocratico o debba essere obbligatoriamente collegiale.	Chiarimento	L'OFG può essere un organo monocratico (cfr. art. 2381, comma 2, c.c. e Disposizioni di vigilanza in materia di organizzazione e governo societario delle banche del 4 marzo 2008, p. 6).

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	Valutazione adeguatezza funzioni di controllo Con riferimento alla previsione di "*assicurare l'adeguatezza delle funzioni aziendali di controllo*" è stato chiesto di chiarire se trattasi di responsabilità anche di valutazione sull'adeguatezza delle funzioni di controllo. Al fine di evitare dubbi, è stato suggerito di precisare che la competenza della valutazione resta in capo all'OFSS.	Sì	Testo modificato.
	Destinatari dei programmi di attività È stato rilevato che non è chiaramente esplicitato, se l'OFG rientri, insieme agli altri organi aziendali, tra i destinatari dei documenti relativi ai programmi di attività delle funzioni di controllo.	Chiarimento	Si conferma che, ai sensi della Sez. III, par. 2, primo alinea, del documento di consultazione, tra i destinatari dei documenti di programmazione e di rendicontazione delle funzioni aziendali di controllo rientra anche l'OFG.
Sezione II (Il ruolo degli organi aziendali), par. 4 (Organo con funzione di controllo)	**OFC e OdV** È stato chiesto di riformulare la disposizione che attribuisce all'OFC le funzioni dell'OdV ex d.lgs. 231/2001 nel senso di riconoscere maggiore flessibilità alla banca nell'assegnare tali funzioni a un organismo appositamente istituito. È stato chiesto di chiarire la natura delle "particolari e motivate esigenze".	In parte	In un'ottica di razionalizzazione del sistema dei controlli della banca si ritiene opportuno, in linea con quanto previsto anche dal codice di autodisciplina di Borsa italiana, prevedere come regola generale, ma derogabile, l'attribuzione delle funzioni dell'OdV all'OFC. Tuttavia, al fine di tener conto delle esigenze di flessibilità organizzativa delle banche, si è modificato il testo, sottolineando il carattere derogabile della disposizione, non solo al ricorrere di particolari esigenze, ma ogniqualvolta la banca sia in grado di motivare la scelta del regime derogatorio.
	Budget OdV	Chiarimento	In generale, gli organismi e le funzioni della banca devono disporre di adeguate risorse, anche

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	È stato chiesto di assegnare all'OFC il budget di spesa a carico dell'ente vigilato generalmente riconosciuto all'OdV.		economiche, per potere svolgere i compiti assegnati. Tale principio si ritiene sia valido anche nel caso di affidamento dei compiti dell'organismo di vigilanza all'organo con funzione di controllo.
	Istituzione dell'OdV È stato chiesto di precisare che l'istituzione dell'OdV è facoltativa.	Chiarimento	Le disposizioni in materia di controlli interni non incidono sulle norme del d.lgs. n. 231/01, che non impongono l'obbligo di istituire l'organismo di vigilanza.
	Remunerazione dell'OdV e dell'OFC È stato chiesto di inserire le seguenti disposizioni con riferimento rispettivamente all'organismo di vigilanza e all'OFC: "*Per lo svolgimento di tali funzioni le banche prevedono un'adeguata remunerazione specifica*."; "*La banca prevede una remunerazione dell'organo con funzioni di controllo adeguata alle dimensioni e alla complessità dell'attività di vigilanza del sistema di controllo interno*."	No	Le tematiche concernenti i criteri di remunerazione degli organi aziendali non sono oggetto del presente documento, ma trattati specificamente nel provvedimento della Banca d'Italia del 30 marzo 2011.
	Comitato per il controllo interno e la revisione contabile, comitato controllo e rischi e OFC È stato chiesto di individuare le modalità di coordinamento tra il comitato controllo e rischi eventualmente istituito in seno al consiglio di amministrazione e il collegio sindacale (o dell'omologo organo di vigilanza nell'ambito dei modelli di amministrazione e controllo alternativi a quello c.d. "tradizionale") investito anche della funzione di comitato per il controllo interno e la	No	Le questioni concernenti il comitato per il controllo interno e la revisione contabile e le modalità di raccordo con altri comitati costituiti all'interno del *board* non sono oggetto delle presenti disposizioni. Esse potranno essere organicamente affrontate, una volta definito il quadro comunitario di riferimento concernente la direttiva 2006/43/CE e la direttiva CRD IV, in occasione della revisione delle disposizioni di vigilanza in materia di organizzazione e governo societario delle banche del 4 marzo 2008 (cfr. programma progetti normativi

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	revisione contabile ex art. 19 del d.lgs. 39/2010. È stato chiesto di individuare le attribuzioni specifiche nell'ambito dei controlli societari bancari al collegio sindacale (o dell'omologo organo di vigilanza nell'ambito dei modelli di amministrazione e controllo alternativi a quello c.d. "tradizionale") investito anche della funzione di comitato per il controllo interno e la revisione contabile ex art. 19 del d.lgs. 39/2010. È stato chiesto di inserire la precisazione che l'OFC svolge altresì le funzioni demandate al Comitato per il controllo interno e la revisione contabile di cui all'art.19 del d.lgs. 39/2010, in quanto le "banche" sono, ai fini del predetto decreto (cfr. art. 16), qualificate come "enti di interesse pubblico".		2012).
Sezione II (Il ruolo degli organi aziendali), par. 5 (Il coordinamento delle funzioni di controllo interne e societarie)	**Compiti dell'OdV** È stato chiesto di eliminare, tra le attività svolte dall'OdV, il riferimento all'adempimento di leggi e regolamenti in quanto tale attività non rientrerebbe tra i compiti dell'organismo.	Chiarimento	L'indicazione che l'attività dell'OdV "*attiene in generale all'adempimento di leggi e regolamenti*" non è diretta a descrivere i compiti dell'organismo (contenuti nel d.lgs. 231/2001), ma a mettere in luce che l'attività di quest'ultimo, essendo di vigilanza sul funzionamento, l'osservanza e l'aggiornamento dei modelli di organizzazione e di gestione adottati per prevenire i reati, è sinergica con quella delle funzioni di *compliance* e di revisione interna di assicurare il rispetto delle leggi e dei regolamenti.
	Ruolo dell'amministratore incaricato del SCI È stato chiesto di eliminare il riferimento alla figura dell'"amministratore incaricato del sistema del controllo interno e di gestione dei rischi" prevista dal Codice di autodisciplina, in quanto la sua istituzione è facoltativa	No	Il testo del documento chiarisce che l'adesione al codice di autodisciplina avviene su base volontaria.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	e potrebbe ingenerare dubbi sulla natura di questa figura di controllo.		
	Modalità di raccordo con i revisori È stato suggerito di definire modalità di raccordo e flussi informativi anche con il soggetto incaricato della revisione legale dei conti e non solo con le funzioni aziendali e societarie.	No	Le presenti disposizioni si focalizzano sul sistema dei controlli interni e disciplinano prevalentemente le modalità di raccordo tra strutture interne alla banca. Si prevede, inoltre, che l'IA, nell'ambito della collaborazione e dello scambio di informazioni con il revisore, individui le criticità emerse durante l'attività e si attivi per rimuoverle (cfr. Sez. II, par. 3.4). Le modalità di raccordo della banca con il revisore esterno potranno essere oggetto di un intervento normativo mirato una volta definiti gli standard internazionali in discussione presso il Comitato di Basilea (cfr. il documento di consultazione *External audits of banks* del marzo 2013).
	Funzioni societarie e interne di controllo È stato chiesto di eliminare i riferimenti alle funzioni di controllo "societarie" e "interne" in quanto potrebbero ingenerare difficoltà interpretative rispetto alla definizione di funzioni aziendali di controllo.	Sì	Testo modificato.
	È stato chiesto di esplicitare il ruolo delle funzioni societarie di controllo con particolare riferimento alla possibile attribuzione di responsabilità analoghe a quelle delle funzioni aziendali di controllo.	In parte	Il riferimento alla disciplina delle funzioni societarie è stato espunto dal testo.
	Nuovi prodotti e impatto su procedure contabili	Sì	Testo modificato.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	È stato chiesto, con riferimento al processo di approvazione di nuovi prodotti, di inserire in capo all'OFG l'obbligo di valutare l'impatto sulle procedure amministrative e contabili per la formazione del bilancio di esercizio e, ove previsto, del bilancio consolidato nonché di ogni altra comunicazione di carattere finanziario.		
	Dirigente preposto È stato chiesto di fornire indicazioni più puntuali circa il ruolo e l'inquadramento della figura del dirigente preposto alla redazione dei documenti contabili societari nell'ambito del sistema dei controlli interni delle banche, con particolare riferimento alla collocazione organizzativa, ai rapporti con le altre funzioni di controllo, alle prerogative di autonomia e indipendenza, ai flussi informativi, ai sistemi di remunerazione e incentivazione.	No	Lo schema di disposizioni disciplina i requisiti di indipendenza e di autonomia nonché i compiti delle funzioni aziendali di controllo. Con riguardo, invece, al dirigente preposto, i cui compiti e responsabilità sono disciplinati nel TUF, si ritiene opportuno che siano le banche, nell'esercizio della propria autonomia organizzativa, a disciplinarne prerogative, collocazione organizzativa e modalità di raccordo con le altre funzioni di controllo; aspetti che devono essere formalizzati nel documento relativo al coordinamento dei controlli interni.
	Istruzioni delle capogruppo estere Nella redazione del documento volto ad assicurare la corretta interazione tra le varie funzioni di controllo, è stato chiesto di tener conto anche degli eventuali indirizzi imposti dalle capogruppo estere e rispondenti a diversi ordinamenti giuridici.	Chiarimento	L'OFSS, nel redigere il documento di coordinamento, può tenere conto degli indirizzi della propria capogruppo estera, sempre che siano compatibili con la normativa italiana.
	Comitato controllo e rischi È stato chiesto di eliminare la precisazione in merito alla composizione del comitato controllo e rischi in quanto solo parzialmente allineata con le previsioni del codice di autodisciplina.	Sì	Testo modificato.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	È stato chiesto di esplicitare nel documento che il ruolo del comitato controllo e rischi è di supporto all'OFSS nelle decisioni concernenti il sistema di controllo interno e di gestione dei rischi.	No	Non si ritiene che questa sia la sede opportuna per disciplinare il ruolo di un comitato, che è rimesso all'autonomia delle banche, tenuto conto della disciplina di vigilanza in materia di *governance* contenuta nelle disposizioni del marzo 2008.
	Documento di coordinamento Con riguardo al "*documento nel quale sono definiti i compiti e le responsabilità di vari organi e funzioni (aziendali e societarie) di controllo (omissis)*", è stato chiesto di rivedere il processo di approvazione proposto (che richiederebbe l'intervento dell'OFSS) che in alcuni casi dovrebbe approvare due volte gli stessi contenuti. Infatti, se una delle finalità è quella di un'analisi sull'andamento dei flussi e sulle aree di sovrapposizione e sinergia, questa – attenendo ad un profilo operativo – potrebbe essere svolta dalle strutture interessate con il coinvolgimento dell'OFG, ferma la reportistica all'organo con funzione di supervisione strategica.	No	Si ritiene che l'approvazione del documento nel quale siano definiti i compiti e le responsabilità nonché le modalità di coordinamento e di collaborazione debba essere di competenza dell'OFSS atteso il suo carattere strategico per il corretto funzionamento del sistema dei controlli inteni. L'eventuale analisi preliminare dei flussi informativi e dell'individuazione delle aree di sovrapposizione sulla base delle quali redigere il documento può essere condotta dall'OFG con il coinvolgimento delle strutture interessate.
Sezione III (Funzioni aziendali di controllo), par. 1 (Istituzione delle funzioni aziendali di controllo)	**Distinzione tra controllo e revisione** È stato chiesto di distinguere, anche a livello definitorio, le funzioni di controllo di secondo livello dalla funzione di revisione interna, che per definizione non esegue attività di controllo in senso stretto, ma appunto attività di revisione (test di funzionalità e conformità).	Chiarimento	Si ritiene che lo schema distingua le funzioni di secondo livello da quelle di terzo livello. In particolare, nella Sezione I, par. 6, sono definiti i controlli di secondo livello e i controlli di terzo livello; nella Sezione III sono descritti i compiti delle singole funzioni di controllo e sono evidenziate le differenze nella natura delle attività svolte da ciascuna di queste.
	Nomina dei responsabili	In parte	Il testo è stato modificato per chiarire che la no-

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	È stato chiesto di chiarire se la disposizione sulla non delegabilità all'OFG del potere di nomina del responsabile delle funzioni di revisione interna e di conformità prevista dal provvedimento della Banca d'Italia sul governo societario sia in contrasto con la disciplina del processo di nomina e revoca dei responsabili delle funzioni di controllo ed è per questo da ritenersi abrogata.		mina e la revoca sono decise dall'OFSS, sentito l'OFC.
	È stato chiesto di prevedere che la nomina del responsabile dell'IA sia deliberata dall'OFSS, previo parere dell'OFC.	Sì	Testo modificato.
	Amministratore delegato con responsabilità di funzioni di controllo È stato chiesto di temperare il divieto di attribuire la responsabilità di una funzione di controllo a un amministratore titolare di deleghe operative in funzione del principio di proporzionalità.	Chiarimento	In generale, i responsabili delle funzioni di controllo non possono avere la titolarità di aree operative sottoposte al proprio controllo. La possibilità di affidare ai responsabili delle funzioni di controllo anche altre aree operative non sottoposte a loro controllo va attentamente valutata alla luce dei principi generali di prevenzione dei conflitti di interesse ed efficacia/efficienza operativa. In base a tali principi, un amministratore potrebbe essere responsabile di una funzione di controllo e al contempo di deleghe operative solo se queste non riguardino attività sottoposte al suo controllo o che possano creare conflitti di interessi.
	Gestione dei reclami e funzione di *compliance* È stato chiesto se la struttura che gestisce i reclami possa essere collocata a riporto funzionale del responsabile della compliance, considerato il divieto di assumere la responsabilità diretta di aree operative.	Chiarimento	La struttura che gestisce i reclami può essere collocata a riporto funzionale del responsabile della *compliance*.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	Accordi di servizio tra IA e *compliance* È stato chiesto di esplicitare la possibilità di utilizzare Accordi di Servizio tra le funzioni di *compliance* e di revisione interna, confermando l'approccio descritto nella Comunicazione congiunta Banca d'Italia - Consob in materia di ripartizione delle competenze tra *compliance* e *internal audit* nella prestazione dei servizi di investimento e di gestione collettiva del risparmio. È stato chiesto se, in linea con quanto previsto dalla Comunicazione congiunta BI-Consob dell'8 marzo 2011 in materia di ripartizione dei compiti fra *compliance* e *internal audit* nella prestazione dei servizi di investimento, la *compliance* possa avvalersi di risorse e funzionalità dell'*internal audit* per l'effettuazione di verifiche in loco.	Chiarimento	Le presenti disposizioni non modificano la citata Comunicazione congiunta che continua ad applicarsi. Più in generale si ritiene che, anche con riferimento alla normativa sui controlli interni delle banche, non vi siano impedimenti alla stipula di tali accordi tra la *compliance* e l'IA.
	Rotazione delle risorse tra le funzioni anziendali È stato chiesto di consentire la rotazione delle risorse non solo all'interno delle singole funzioni, ma anche tra le diverse funzioni aziendali di controllo.	Sì	Testo modificato.
	È stato chiesto che sia prevista una formalizzazione della politica aziendale in materia di rotazione delle risorse.	Sì	Testo modificato.
	Requisiti di professionalità È stato chiesto di esplicitare i requisiti di professionalità che dovrebbero avere i responsabili delle funzioni di controllo.	No	La valutazione della professionalità dei titolari delle funzioni di controllo è rimessa all'autonomia organizzativa della banca che assume la responsabilità delle scelte effettuate.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	Politiche di remunerazione È stato chiesto di richiamare le responsabilità in materia di determinazione delle remunerazioni dei responsabili delle funzioni di controllo nella disciplina sulle politiche di remunerazione.	Chiarimento	I criteri per la determinazione delle remunerazione dei componenti delle funzioni aziendali di controllo sono stabiliti nel Provvedimento della Banca d'Italia del 30 marzo 2011 in materia di politiche e prassi di remunerazione e incentivazione nelle banche e nei gruppi bancari.
	Ruolo della capogruppo nella nomina/revoca dei responsabili È stato chiesto di integrare la previsione sulla nomina e la revoca dei responsabili delle funzioni di controllo con il parere delle omologhe funzioni di gruppo.	No	La nomina dei responsabili delle funzioni di controllo spetta agli organi aziendali secondo le rispettive competenze e nell'interesse della società. Eventuali pareri o proposte di altri soggetti appartenenti al gruppo possono essere previsti nell'ambito delle procedure di coordinamento formalizzate dalla capogruppo, ferma restando la responsabilità degli organi aziendali.
	Accorpamento RM e *compliance* È stato chiesto se le banche siano tenute a nominare un responsabile della *compliance* nei casi in cui l'attività di controllo della conformità sia affidata al *risk management*.	Chiarimento	Nei casi in cui, in applicazione del principio di proporzionalità, il RM e la *compliance* sono accorpati, dovrà essere nominato un unico soggetto che assume la responsabilità di entrambe le funzioni.
	Responsabilità referente È stato chiesto di chiarire se nel caso di esternalizzazione delle funzioni aziendali di controllo, la responsabilità della funzione di controllo sia attribuita al referente.	Chiarimento	Il referente è responsabile del controllo delle singole attività esternalizzate e, di conseguenza, del corretto funzionamento della funzione esternalizzata. Resta ferma, in ogni caso, la responsabilità degli organi aziendali.
	Autorizzazione per l'applicazione del principio proporzionalità È stato proposto, in linea con quanto avviene in altri	No	Le disposizioni di vigilanza, in alcune circostanze, graduano le previsioni normative tenuto conto delle caratteristiche degli intermediari (es.: cate-

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	ordinamenti, di prevedere che l'applicazione del principio di proporzionalità sia autorizzata dalla Banca d'Italia.		gorie di intermediari che possono ricorrere all'esternalizzazione di funzioni aziendali di controllo); in altre circostanze, è rimesso all'autonomia degli intermediari applicare le norme in funzione del principio di proporzionalità, fermo restando che la Banca d'Italia valuta la corretta applicazione del principio.
	Definizione di aree operative e di funzioni di staff Con riferimento alla previsione secondo cui "*i responsabili di tali funzioni non devono avere responsabilità diretta di aree operative né devono essere gerarchicamente subordinati ai responsabili di tali aree*", è stato chiesto di chiarire la definizione di "aree operative", specificando se tra le aree operative si intenda anche l'attività di erogazione creditizia. È stato chiesto se, in caso di entità di piccole dimensioni, il responsabile della *compliance* possa essere anche il responsabile delle risorse umane. È stato chiesto se l'indipendenza dei responsabili delle funzioni di controllo dalle aree operative includa anche l'indipendenza dalle aree che svolgono funzioni di staff.	Chiarimento	In generale, i responsabili delle funzioni di controllo non possono avere la titolarità di aree operative sottoposte al proprio controllo, quale, ad es., l'erogazione creditizia; né essi possono riportare ai responsabili di dette attività. Con riferimento alle funzioni di staff, la possibilità di affidarle ai responsabili delle funzioni di controllo va attentamente valutata alla luce dei principi generali di prevenzione dei conflitti di interesse e di efficacia/efficienza dei processi aziendali.
	Parere del comitato controllo e rischi sulla nomina dei responsabili delle funzioni di controllo È stato chiesto di prevedere l'acquisizione del parere del comitato controllo e rischi anche per la nomina e revoca dei responsabili delle funzioni aziendali di controllo.	Chiarimento	Le disposizioni non prevedono un obbligo in tal senso; tuttavia, le banche, nell'ambito della propria autonomia organizzativa, hanno la facoltà di prevedere il parere del comitato controllo e rischi sulla nomina e sulla revoca dei responsabili delle funzioni di controllo.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
Sezione III (Funzioni aziendali di controllo), par. 2 (Programmazione e rendicontazione dell'attività di controllo)	**Programma di attività** Con riguardo al programma di attività, è stato chiesto di precisare i criteri che ogni singola banca potrà seguire per identificare il contenuto dello stesso, tenendo in considerazione che le funzioni di conformità alle norme e di controllo dei rischi hanno tra i loro compiti anche attività ulteriori rispetto agli interventi programmati in funzione dell'attività di identificazione e valutazione dei rischi.	Chiarimento	Fermi restando i compiti delle funzioni previsti nelle rispettive disposizioni, il programma, con approccio *risk based*, ha la finalità di fissare le priorità tra le attività da svolgere e di rappresentare ai vertici gli aspetti di maggior rilevo che impegneranno le funzioni.
	È stato chiesto di distinguere tra l'attività di programmazione del *risk management* e quella delle altre funzioni di controllo, in considerazione del fatto che il RM opera nel continuo, coprendo tutte le aree di processo e di rischio.	No	L'attività del *risk management*, pur svolgendosi nel continuo ed estendendosi a tutte le aree di rischio, non preclude la possibilità di programmare annualmente la propria attività tenuto conto delle carenze riscontrate, della rilevanza di determinati rischi e dei nuovi rischi cui la banca sarà eventualmente esposta in funzione delle scelte gestionali pianificate.
	È stato chiesto di chiarire il contenuto minimo della specifica sezione relativa all'attività di revisione interna del sistema informativo (ICT auditing), in quanto una mera elencazione nel piano operativo degli interventi di audit pianificati potrebbe risultare una forma di rappresentazione non sufficientemente conforme con quanto espressamente richiesto nel documento.	Chiarimento	Si ritiene che, come ogni altro aspetto del piano, la sezione relativa all'ICT auditing debba avere il livello di dettaglio necessario a consentire agli organi aziendali di valutare le attività da svolgere al fine di adottare le relative deliberazioni.
	Distinzione tra affidabilità e funzionalità È stato chiesto di chiarire la differenza tra affidabilità (pag. 17) dello SCI e funzionalità (pag. 10) dello stesso.	Sì	Testo modificato per allineare la terminologia.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	Laddove si prevede che le funzioni di controllo "*riferiscono, ciascuna per gli aspetti di rispettiva competenza, in ordine alla completezza, adeguatezza ed affidabilità del sistema dei controlli interni*", è stato chiesto di chiarire se il termine "affidabilità" sia da intendersi quale sinonimo di "funzionalità", termine impiegato in altri casi, o in generale di "efficacia".		
	Relazione della funzione convalida È stato chiesto se la relazione annuale della funzione di controllo dei rischi possa contenere anche l'informativa annuale che deve rendere la funzione di convalida senza che siano previste due relazioni distinte.	Chiarimento	Si, la relazione della funzione di controllo dei rischi può ricomprendere quella dovuta dalla funzione di convalida.
	Oneri di rendicontazione È stato chiesto di semplificare e proporzionalmente ridurre le richieste regolamentari e di rendicontazione riferite a intermediari di dimensione contenuta o contrassegnati da limitata complessità operativa e bassa propensione al rischio.	No	Il documento indica espressamente i casi in cui può essere applicato il principio di proporzionalità. L'obbligo di rendicontazione non può venir meno; tuttavia, l'entità della rendicontazione richiesta per assolvere gli obblighi imposti è essa stessa connessa alla dimensione e al grado di complessità operatività di ogni banca.
	È stato chiesto di rafforzare gli obblighi informativi di carattere periodico del RM nei confronti degli organi aziendali in luogo della rendicontazione annuale.	Chiarimento	La regolamentazione dei flussi informativi periodici è rimessa alla regolamentazione interna, fermo restando l'obbligo di informare nel continuo gli organi aziendali sia dell'evoluzione dei rischi aziendali, sia di eventuali violazioni o carenze riscontrate nell'attività di controllo. Si ritiene che la rendicontazione annuale sia uno strumento aggiuntivo utile per gli organi aziendali al fine di valutare l'andamento complessivo del

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
			sistema dei controlli interni e valutare possibili miglioramenti strategici non legati esclusivamente alla risoluzione di singole criticità.
	Relativamente ai flussi informativi richiesti a ciascuna funzione aziendale di controllo, è stato suggerito – per maggiore chiarezza – di specificare che il programma di attività, la relazione dell'attività svolta e la situazione dei controlli interni, possano essere contenuti anche in un singolo documento (ad es., come avviene già con il documento interno annuale della funzione di *compliance*).	Chiarimento	Si conferma che ciascuna funzione può presentare un documento unitario che includa il programma di attività (per l'IA, il piano audit), la relazione sull'attività svolta nell'anno precedente e le considerazioni in merito alla completezza, adeguatezza, funzionalità e affidabilità del sistema dei controlli interni.
Sezione III (Funzioni aziendali di controllo), par. 1 (Istituzione delle funzioni aziendali di controllo) e 3.3 (Funzione di controllo dei rischi)	**Collocazione del RM e della *compliance*** È stato chiesto di specificare se, con riferimento alla collocazione della funzione di *risk management*, la locuzione "*alle dirette dipendenze*" debba essere in senso di "*collocazione gerarchica*" o di "*riferiscono direttamente*". È stato chiesto di equiparare, in termini di collocazione gerarchica e linee di riporto il ruolo della *compliance* a quello del *risk management*. È stato proposto di prevedere un riporto congiunto all'amministratore delegato e agli organi collegiali da parte del responsabile della funzione di controllo dei rischi.	In parte	Testo modificato. Al fine di contemperare l'autonomia organizzativa delle banche con l'esigenza di preservare l'autorevolezza delle funzioni di controllo, la disposizione in parola è stata modificata prevedendo che le funzioni di controllo di secondo livello riportino gerarchicamente all'OFG, ferma restando la possibilità per la banca di collocare tali funzioni alle dipendenze dell'OFSS.
	È stato chiesto di chiarire se il collocamento delle funzioni di controllo alle dirette dipendenze del comitato controllo e rischi:	In parte	Il testo è stato modificato per chiarire che le funzioni di controllo, inclusa la *compliance*, se non poste alle dipendenze dell'OFG, possano essere collocate gerarchicamente a riporto dell'OFSS e

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	- sia obbligatorio, ove tale comitato sia costituito; - comporti un trasferimento di responsabilità dal plenum al comitato. È stato chiesto di attribuire il medesimo rango organizzativo a tutte le funzioni di secondo livello.		non del comitato controllo e rischi.
	Partecipazione RM a comitati del board È stato chiesto di definire nel dettaglio le modalità di partecipazione della funzione di controllo dei rischi ai comitati istituiti nel *board*.	Chiarimento	Si ritiene, in generale, che sia opportuna la diretta partecipazione dei responsabili delle funzioni di controllo ai comitati del *board*. Tuttavia, le modalità di tale partecipazione sono rimesse all'autonomia organizzativa della banca.
	Collocazione del CRO È stato chiesto di riconoscere la possibilità che venga istituita una figura di supervisione e coordinamento di autonome e separate funzioni aziendali (c.d. CRO). È stata altresì chiesta una valutazione/interpretazione dei possibili ruoli delle diverse funzioni di controllo e delle reciproche interrelazioni in presenza del CRO. Infine, è stato chiesto di riconoscere esplicitamente nel documento la possibilità che al CRO riportino gerarchicamente sia il responsabile della funzione *risk management*, sia quello della funzione *compliance* e ciò in quanto: - favorirebbe un approccio maggiormente integrato alla gestione dei rischi; - vi sarebbero strette interrelazioni tra il potere di fornire pareri preventivi del *risk management* e le valutazioni *ex-ante* tipicamente effettuate	No	In linea con quanto stabilito dalle linee guida internazionali (cfr., tra l'altro, EBA *Guidelines on internal governance*; FSB *Thematic Review on Risk Governance*), la Banca d'Italia identifica il CRO con il responsabile della funzione *risk management* che, in quanto tale, non può essere sovraordinato gerarchicamente al responsabile della funzione *compliance*, fatto salvo il principio di proporzionalità. Le due funzioni, infatti, essendo entrambe di secondo livello e richiedendo professionalità tra loro eterogenee, sebbene complementari, devono conservare una certa indipendenza reciproca e autonomia di giudizio. Per quanto concerne, invece, la possibilità di istituire una figura di coordinamento dei controlli di secondo livello, cui riportano gerarchicamente i responsabili delle funzioni di secondo livello, la Banca d'Italia ritiene non compatibile l'istituzione di tale figura con l'assetto del sistema dei control-

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	dalla *compliance*; - si garantirebbe una maggiore flessibilità organizzativa. Nel caso in cui sia prevista la figura del CRO si chiede che venga esclusa la possibilità che la funzione di *compliance* dipenda gerarchicamente direttamente da questa figura.		li. L'istituzione di siffatta figura a livello aziendale provocherebbe, in sostanza, la creazione di un ulteriore livello tra le funzioni di secondo livello e l'OFG cui queste riportano gerarchicamente con il rischio che la dialettica diretta tra OFG e funzioni di controllo venga filtrata dal soggetto intermedio. Naturalmente ciò non vieta che all'interno dell'OFG o dell'OFSS venga specificatamente individuato un amministratore che assuma il ruolo di coordinamento delle funzioni aziendali di controllo in linea anche con quanto previsto dal codice di autodisciplina di Borsa italiana.
Sezione III (Funzioni aziendali di controllo), par. 3.2 (Funzione di conformità alle norme)	**Compiti della funzione di conformità alle norme** Si suggerisce di chiarire come debba essere interpretata la frase "*presiedere alla gestione*" del rischio di non conformità contenuta nelle disposizioni. Se tale locuzione è da intendersi nel senso di prevedere una responsabilità ultima della funzione di conformità per tutte le normative che hanno impatto aziendale, si osserva che non è operativamente praticabile in molte realtà, soprattutto di minori dimensioni, ed è spesso in contrasto con il principio di economicità. **Perimetro** Si richiede di chiarire il perimetro di competenza e la responsabilità della funzione di *compliance* per quelle normative che non regolano o non sono direttamente attinenti allo svolgimento dell'attività bancaria, per le	In parte	Testo modificato. Con riferimento alla questione del perimetro della *compliance*, è stato chiarito che – ferma restando l'estensione del rischio di non conformità presidiato dalla *compliance* a tutte le disposizioni applicabili alle banche - il coinvolgimento della funzione di compliance deve essere proporzionale al rilievo che le singole norme hanno per l'attività svolta e alle conseguenze della loro violazione. Ciò significa che il coinvolgimento della funzione dovrà essere massimo per l'attività di prevenzione e gestione del rischio di violare le norme in materia di attività bancaria e servizi di investimento, di gestione dei conflitti di interesse, di trasparenza nei confronti del cliente e, più in generale, di tutela del consumatore. Su tali aree, la *compliance* può essere considerata il principale

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	quali la normativa settoriale prevede la presenza di specifiche figure di riferimento e garanzia (ad es., normativa *privacy*, responsabile della sicurezza). **Perimetro: processi di vigilanza prudenziale** Si chiede che vengano chiariti ruoli e responsabilità della *compliance* e delle diverse funzioni specialistiche coinvolte nei processi rilevanti per la vigilanza prudenziale, fermo restando il riconoscimento dell'autonomia organizzativa delle banche.		*owner* del rischio ed è chiamata a dotarsi delle professionalità necessarie e a definire appositi raccordi con altre funzioni di controllo - anche con specifici accordi di servizio - per garantire un presidio continuo ed efficace dei processi. Diversamente, in relazione ad altre normative, per le quali siano già previste forme specifiche di presidio specializzato all'interno della banca, il coinvolgimento della funzione di *compliance*, sempre basato su un approccio *risk-based*, può essere meno intenso ma mai assente. In sostanza, la funzione sarà chiamata a collaborare alla predisposizione delle procedure necessarie ad assicurare il rispetto delle norme e a verificare il loro corretto funzionamento. Con riferimento alle norme tributarie, il ruolo della *compliance* può limitarsi alla definizione di procedure che, per quanto possibile, pongano la banca al riparo dalle conseguenze, sia sanzionatorie sia reputazionali, di una loro violazione (prevedendo il ricorso a figure interne alla banca esperte in materia fiscale ovvero, nei casi più complessi, l'acquisizione del parere delle autorità tributarie competenti). La successiva applicazione di tale procedura può non rientrare nell'ambito di competenza della funzione di *compliance*, che è soltanto tenuta a verificare che le procedure realizzino effettivamente l'obiettivo di gestione e attenuazione del rischio al quale erano dirette. In conclusione, ricade nella responsabilità del *chief compliance officer* la predisposizione delle procedure e la verifica del loro corretto funzionamento con riferimento a tutte le norme che si ap-

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
			plicano alla banca.
	Perimetro: norme fiscali Si propone di attendere la legge delega per il riordino della materia fiscale che dovrebbe prevedere l'obbligo di introdurre sistemi aziendali di gestione e controllo dei rischi di natura tributaria. Con riferimento al rischio fiscale, l'attuazione della delega potrebbe portare a indicazioni contrastanti con quelle contenute nelle nuove istruzioni di vigilanza sui controlli interni.	No	Si ritiene che le disposizioni di vigilanza siano coerenti con la legge delega sul riordino in materia fiscale per quanto riguarda il sistema di controllo dei rischi di natura tributaria; d'altra parte, l'incertezza dei tempi di approvazione della legge delega e dei relativi decreti attuativi non rende opportuno attendere la definizione del nuovo quadro normativo. In ogni caso, sarà curato con la massima attenzione il coordinamento delle due discipline.
	Si propone di chiarire la previsione secondo la quale le banche devono tener conto dei rischi derivanti dal coinvolgimento in operazioni fiscalmente irregolari poste in essere dalla clientela. La banca presidia il rischio derivante dalle operazioni fiscalmente irregolari della clientela con i presidi derivanti essenzialmente dalla normativa antiriciclaggio e può tener conto dei rischi di operazioni fiscalmente irregolari da parte dei clienti solo nel caso offra specifica consulenza su particolari operazioni richieste dai clienti stessi.	Chiarimento	Il compimento di operazioni per conto della clientela in violazione/elusione di norme fiscali espone la banca a rilevanti rischi, anche di natura reputazionale. La banca deve adottare ogni cautela per evitare di essere coinvolta in operazioni di tale natura, anche tenuto conto del livello di diligenza professionale cui è tenuta.
	***Compliance* negli intermediari minori** Per gli intermediari minori, si chiede di prevedere la facoltatività dell'inserimento in capo alla funzione di *compliance* della verifica di conformità dell'attività aziendale alle normative di natura fiscale e di declinare nel testo delle disposizioni l'ambito rimesso alla libertà organizzativa per gli intermediari, prevedendo la possibilità di porre in essere forme di collaborazione tra la	In parte	I compiti e i principi di riferimento della funzione di *compliance* sono uguali per tutti gli intermediari a prescindere dalle dimensioni. Coerentemente con tali principi sono consentite forme di collaborazione tra la funzione specialistica tributaria e la funzione di *compliance* per monitorare e prevenire il rischio di non conformità alle norme fiscali.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	funzione specialistica tributaria, ovunque allocata, e la funzione *compliance*, che non risulta nella generalità dei casi dotata del necessario bagaglio di conoscenze specialistiche.		
	Posizionamento organizzativo Si chiede di prevedere che la funzione di *compliance* debba avere un posizionamento organizzativo tale da assicurare l'accesso diretto all'organo con funzione di supervisione strategica o al comitato specializzato costituto al suo interno.	Sì	Testo modificato.
Sezione III (Funzioni aziendali di controllo), par. 3.3 (Funzione di controllo dei rischi)	**Parere su operazioni rilevanti** È stato chiesto di integrare la previsione secondo cui la funzione di controllo dei rischi «*dà pareri preventivi sulla coerenza con la politica di governo dei rischi delle operazioni di maggiore rilievo*», inserendo il seguente periodo finale «*eventualmente acquisendo, in funzione della natura della operazione, il parere di altre funzioni interne coinvolte nel processo di gestione dei rischi (ad es. funzione di compliance, funzione ICT)*».	Sì	Testo modificato.
	Esplicitazione attribuzioni del RM È stato chiesto di arricchire l'elencazione dei compiti delle funzioni di controllo dei rischi con l'esplicitazione di alcune attribuzioni che risulterebbero al momento solo sottese all'impianto del Documento, quali ad es.: – la definizione di metriche comuni di valutazione dei rischi operativi, coerenti con le politiche di governo dei rischi, coordinandosi con le funzioni di controllo di conformità e le funzioni ICT	Sì	Testo modificato.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	della banca; – la definizione di modalità di valutazione e controllo dei rischi reputazionali, coordinandosi con le funzioni della banca che in primo luogo sono chiamate a gestire tali tipologie di rischio (funzioni di comunicazione, *investor relations*, ecc.); – il supporto ai competenti organi della banca ai fini della valutazione del rischio strategico, tenuto anche conto di variabili esogene a valenza significativa (ad es., evoluzione normativa in specifici settori di *business*; variabili macroeconomiche per aree geografiche; tendenze demografiche; riforme ad impatto sistemico); – la verifica sulla coerenza dei sistemi di misurazione e controllo dei rischi con i processi e le metodologie di valutazione, anche a fini contabili, delle attività aziendali, coordinandosi con le strutture aziendali a vario titolo coinvolte nei suddetti processi.		
	Indicatori di anomalia È stato chiesto di eliminare il requisito che richiede di sviluppare un sistema di indicatori di anomalia o inefficienza dei sistemi di misurazione dei rischi.	No	Si ritiene opportuno che vengano sviluppati indicatori di anomalia o inefficienza dei sistemi di misurazione dei rischi al fine verificare nel continuo l'affidabilità dei sistemi impiegati.
	Valutazione ex post delle operazioni di maggior rilievo È stato chiesto di valutare una proposta alternativa di previsione normativa secondo cui il RM verificherebbe	Chiarimento	Il parere preventivo sulle operazioni di maggior rilievo è una misura di *escalation* volta a coinvolgere gli organi aziendali su determinate operazioni, normalmente di competenza delle funzioni di *business* che, per i particolari profili di rischio,

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	ex-post, e non *ex ante*, le operazioni di maggior rilievo.		sono ritenute dal RM meritevoli di particolare attenzione.
Sezione III (Funzioni aziendali di controllo), par. 3.4 (Funzione di revisione interna)	**Trasmissione degli esiti degli accertamenti** Con riferimento all'obbligo di trasmissione agli organi aziendali degli esiti degli accertamenti conclusisi con giudizi negativi o che evidenzino carenze di rilievo, è stato suggerito di eliminare "di rilievo" riferito solo alle carenze e di inserire all'inizio della frase "nel caso di rischi rilevanti".	No	Si ritiene opportuno che tutti i giudizi negativi siano trasmessi agli organi aziendali.
	Definizione attività rilevanti Sono stati richiesti chiarimenti/esempi circa la definizione di attività rilevanti o indicazioni su quale debba essere l'organo/funzione aziendale deputato alla definizione e/o alla approvazione di tali attività. Si richiede, inoltre, se per la definizione di tali attività rilevanti debbano essere presi a riferimento i parametri indicati nella definizione di "Funzione operativa importante".	Chiarimento	Nel documento è riportato un esempio di attività rilevante (l'attività di elaborazione dei dati). Spetta alla funzione di revisione interna stabilire in modo autonomo e indipendente quali attività siano rilevanti per il funzionamento del sistema dei controlli interni; i parametri riportati nella definizione di "Funzione operativa importante" possono costituire un utile riferimento per l'identificazione delle attività rilevanti, ma non costituiscono gli unici aspetti da tenere in considerazione.
	Ruolo dell'IA per la determinazione della *risk tolerance* È stata segnalata l'opportunità di ben distinguere, in tema di *risk appetite/tolerance*, il ruolo della funzione di controllo dei rischi - che propone e supporta le decisioni degli organi di vertice in merito alle scelta in materia di *risk appetite* e di conseguente declinazione di *risk tolerance* - da quello attribuito alla funzione di revisione interna.	Chiarimento	Nel documento appare chiara la distinzione tra il ruolo della funzione di controllo dei rischi nel proporre e supportare le decisioni degli organi aziendali in materia di *risk appetite* (attività ex ante) rispetto al ruolo della funzione di revisione interna che valuta la conformità dell'operatività aziendale al *risk appetite* definito dall'organo con funzione di supervisione strategica (attività *ex post*).

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	Applicazione degli standard internazionali È stato suggerito di prevedere nel paragrafo dedicato alla funzione di revisione interna, un richiamo all'opportunità di rifarsi agli standard internazionali di *internal audit*, anche sulla base di quanto espresso nel documento "*The internal audit function in banks*", giugno 2012, Comitato di Basilea.	Sì	Testo modificato.
	Approvazione del piano *audit* da parte dell'OFSS È stato suggerito di prevedere che l'OFSS debba approvare il piano annuale di *audit* e non solo esaminarlo. E' stato proposto pertanto di modificare il testo come segue "*la funzione di revisione interna presenta annualmente agli Organi aziendali un piano di audit per la relativa approvazione*".	Sì	Testo modificato.
	Rotazione del personale È stata accolta con favore l'introduzione del concetto della rotazione del personale (sia internamente che da/per altre aree funzionali della banca), tuttavia è stato chiesto che la rotazione del personale sia regolata e condotta in conformità con una sana politica scritta coerentemente con quanto rimarcato dal Comitato di Basilea.	Sì	Testo modificato.
	Valutazione dei processi di *governance* dei rischi È stato proposto di riprendere nella descrizione delle attività e del ruolo della funzione alcuni passaggi del documento del Comitato di Basilea '*The Internal Audit function in banks*' (giugno 2012). In particolare, andrebbe data maggiore enfasi al compito di valutare, in	Sì	Testo modificato.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	via generale, qualità ed efficacia dei sistemi e processi aziendali di governance dei rischi.		
	Relazione dell'IA con autorità di vigilanza È stato altresì chiesto, sulla scorta di quanto previsto dal documento di Basilea, di richiamare ed enfatizzare i principi di relazione della funzione di IA con l'autorità di vigilanza.	No	La presenti disposizioni si focalizzano prevalentemente sull'assetto dei controlli interni delle banche. I principi richiamati nel documento di Basilea, relativi alle relazioni tra funzione di revisione interna e *supervisor*, esulano dall'oggetto delle presenti disposizioni in quanto riguardano prassi di vigilanza.
	Pianificazione *risk based* Per enfatizzare l'importanza che la pianificazione dell'attività debba essere strettamente correlata ai rischi, è stato suggerito di integrare la disciplina come segue: "*La frequenza delle ispezioni deve essere coerente con l'attività svolta e il relativo livello di rischio*".	Sì	Testo modificato.
	Riparto di competenze tra IA e *compliance* Nel Documento è riportato che la funzione di revisione interna verifica il rispetto delle norme da parte di tutti i livelli aziendali; considerato che il Documento demanda alla funzione di *compliance* il compito di verificare che le procedure interne siano coerenti con l'obiettivo di prevenire la violazione di norme esterne (leggi e regolamenti) o di autoregolamentazione applicabili alle banche, è stato segnalato che potrebbe emergere una possibile area di sovrapposizione con la funzione di *compliance*. È stato pertanto richiesto di meglio precisare il perimetro di attribuzione dei controlli ex post sulle norme per le funzioni di *compliance* e *internal audit*.	Chiarimento	Il ruolo della *compliance* è quello di assicurare che le procedure interne siano adeguate al fine di rispettare la normativa applicabile; per tale finalità, la *compliance* può effettuare controlli *ex-post* sulle procedure interne ovvero concordare con l'IA l'effettuazione di tali controlli da parte di quest'ultima. Il documento di coordinamento dovrà stabilire le modalità di raccordo tra le due funzioni e i relativi flussi informativi per assicurare l'efficace svolgimento delle attività di controllo. Rimangono ferme le responsabilità dell'IA di verificare, in ottica di terzo livello, la robustezza

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
			complessiva del sistema dei controlli interni anche con riferimento al rispetto delle norme.
	Controllo del piano del fornitore di servizi È stato chiesto di chiarire cosa debba intendersi per "coinvolgimento" nel controllo dei piani di continuità operativa dei fornitori di servizi e dei fornitori critici da parte della funzione di revisione interna.	Sì	Testo modificato.
	Collocazione del responsabile dell'IA È stata condivisa la collocazione organizzativa del responsabile della funzione di *internal audit* prospettata nel Documento; tuttavia, è stato rilevato che attribuire all'OFG le prerogative "*al fine di concorrere all'indirizzo dell'attività di revisione interna*" possa rappresentare un pregiudizio all'indipendenza della funzione medesima, in particolare con riferimento alle banche che adottano un sistema di *governance* tradizionale, poiché l'OFG viene nella maggioranza dei casi a identificarsi con la figura dell'amministratore delegato, soggetto a sua volta all'attività di *auditing*. È stato pertanto proposto di modificare il testo eliminando la locuzione "*al fine di concorrere all'indirizzo dell'attività di revisione interna*".	Sì	Testo modificato.
	Flussi tra l'IA e le altre funzioni Con riferimento ai rapporti tra le funzioni aziendali di controllo e le altre funzioni aziendali, è stato suggerito di inserire un principio di reciprocità nello scambio dei flussi tra l'*internal audit* e le altre funzioni di controllo**.**	Sì	Testo modificato.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	Ambito di azione dell'IA Sono stati sollevati alcuni dubbi sulla previsione che prevede verifiche sulle attività aziendali: ciò comporterebbe di fatto controllare tutto l'attivo di bilancio. Si porrebbe, pertanto, una criticità in ordine alle competenze e all'impegno richiesti alla funzione e si ravvisa una duplicazione di attività con i compiti del revisore e con le determinazioni contabili e di bilancio.	No	Ove si prevede che la funzione di revisione interna effettua la valutazione delle regolarità delle diverse attività aziendali, il concetto di attività aziendali non è da intendersi come attività contabili ma come "azioni" poste in essere dalla banca.
	Andamenti anomali È stato proposto di eliminare la specifica previsione che prevede per la funzione di revisione interna il compito di individuare "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 nella sostanza attribuisce a funzioni di controllo di secondo livello, 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.	Sì	Testo modificato
	Verifica del piano di continuità operativa È stato suggerito di lasciare in capo alla revisione interna l'obbligo di una verifica che abbia ad oggetto il piano aziendale di continuità operativa, ma di attribuire l'obbligo di assistere alle relative prove e di controllarne	No	Tenuto conto della rilevanza del piano di continuità operativa, si ritiene che l'IA debba avere un ruolo attivo nel valutare l'adeguatezza del piano e non limitarsi ad esaminare i programmi di verifica, i risultati delle prove, i piani di continuità ope-

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	i risultati a strutture più propriamente interessate a verifiche di prossimità e di natura permanente.		rativa dei fornitori di servizi e dei fornitori critici.
	Flussi informativi tra l'IA e il revisore contabile Il Documento prevede, da parte della funzione di revisione interna, collaborazione e scambio di informazioni con il soggetto incaricato della revisione legale dei conti. È stato suggerito - 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 - di valutare se la modalità operativa da esperire affinché le competenti funzioni aziendali adottino i presidi necessari per superare tale criticità, non possa essere assegnata in generale alla banca (che declinerà in base al proprio modello di funzionamento) piuttosto che alla revisione interna.	No	Si ritiene che lo scambio di informazioni tra la funzione di *internal audit* e il revisore contabile sia essenziale per assicurare effettività ai due momenti di controllo. Tra l'altro, si fa presente che i principi di revisione contabile raccomandati dalla Consob prevedono l'obbligo per il revisore legale di acquisire informazioni dalla funzione di revisione interna.
	Con riferimento alla seguente previsione: *"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"*, è stato evidenziato 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.	In parte	Gli obblighi di comunicazione della società di revisione sono disciplinati dal d.lgs. 39/2010 che prevede un "*duty to report*" al comitato per il controllo interno e la revisione legale. L'IA può comunque venire a conoscenza di criticità emerse durante la revisione legale nell'ambito della collaborazione e dello scambio di informazioni con il soggetto incaricato della revisione legale dei conti. La disposizione è stata pertanto modificata per chiarire tali aspetti.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	Riporto dell'IA di banche controllate verso la capogruppo Al fine di rafforzare i raccordi dell'IA delle banche controllate con le omologhe funzioni di capogruppo, è stato proposto 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*".	No	Fermo restando quanto previsto in materia di esternalizzazione nell'ambito dei gruppi, l'IA dipende gerarchicamente dall'OFSS. Ciò è in linea con quanto previsto dal documento del Comitato di Basilea '*The Internal Audit function in banks*' che prevede che "*the bank has its own internal audit function, which should be accountable to the bank's board and should report to the banking group or holding company's head of internal audit*". Pertanto si ritiene di mantenere l'attuale testo che prevede la dipendenza gerarchica dall'OFSS, fermo restando tutti gli altri obblighi di riporto all'omologa funzione di gruppo.
	Adeguatezza delle risorse Con riferimento ai seguenti compiti assegnati alla funzione di revisione interna: "*Con specifico riferimento al processo di gestione dei rischi, la funzione di revisione interna valuta: l'organizzazione, i poteri e le responsabilità della funzione di controllo dei rischi, anche con riferimento alla qualità e all'adeguatezza delle risorse a questa assegnate;*" è stato osservato che il termine generico di "risorse" potrebbe essere inteso come riferibile anche alle "risorse umane" interpretando tale disposizione come l'assegnazione alla funzione di revisione interna del compito di valutazione dei profili di	No	L'IA, nell'ambito dei propri compiti di valutazione della completezza, dell'adeguatezza, della funzionalità e dell'affidabilità del sistema dei controlli interni, è tenuto anche a valutare l'adeguatezza delle risorse, incluse quelle umane, delle funzioni aziendali di controllo. Tale compito non si sovrappone con quello degli organi aziendali di assicurare (e non solo di valutare) l'adeguatezza delle risorse assegnate a tali funzioni.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	competenza e capacità professionale del personale incaricato della funzione di controllo dei rischi; tali compiti risultano, invece, esplicitamente assegnati all'organo di supervisione strategica (cfr. Sez. II par 2: "*L'organo con funzione di supervisione strategica si assicura, inoltre, che le funzioni aziendali di controllo possiedano i requisiti previsti nella Sezione III*") e all'organo con funzione di gestione (cfr. Sez. II par 3: " *… assicura, altresì, che le attività rilevanti siano dirette da personale qualificato, con adeguato grado di autonomia di giudizio e in possesso di esperienze e conoscenze adeguate ai compiti da svolgere;"*) nonché all'organo con funzione di controllo (cfr. Sez. II par 4: "*l'organo con funzione di controllo è tenuto ad accertare l'adeguatezza di tutte le funzioni coinvolte nel sistema dei controlli,*"). È stato chiesto, pertanto, di precisare che trattasi di "*risorse organizzative e tecnologiche",* al fine di evitare possibili improprie interpretazioni.		
	Divieto incarichi a membri IA esternalizzata Con riguardo ai presidi per prevenire situazioni di conflitto di interessi più volte richiamati all'interno della disciplina, e alle prescrizioni volte ad assicurare l'indipendenza delle funzioni aziendali di controllo (Sez. III, par. 1), è stato osservato che il principio esposto alla lettera c) ("*il personale che partecipa alle funzioni aziendali di controllo non sia coinvolto in attività che tali funzioni sono chiamate a controllare.*") meriterebbe di essere completato con un esplicito riferimento al divieto di assegnazione di incarichi/attività di consulenza al personale facente parte della struttura esterna incaricata di svolgere l'attività di revisione interna "esternalizza-	Sì	Testo modificato.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	ta" (*internal audit*), come peraltro previsto dal documento "*The internal audit function in banks*", June 2012 del Basel Committee on Banking Supervision (Principle 15).		
	Accertamento di specifiche irregolarità È stato chiesto di eliminare l'inciso "*ove richiesto dagli organi aziendali*" nella frase in cui si richiede che la funzione di revisione interna espleti compiti d'accertamento anche con riguardo a specifiche irregolarità.	Sì	Testo modificato.
	Verifiche su attività esternalizzate È stato chiesto di chiarire se la verifica sulle attività esternalizzate debba intendersi come analisi direttamente svolta dalla funzione di revisione interna su tutti i processi in *outsourcing* o può prendere a riferimento le verifiche svolte anche da altre strutture aziendali per il controllo dello svolgimento delle stesse, ove tali strutture esistano.	Chiarimento	Nel documento è chiaramente riportato che: - tutte le attività aziendali, incluse quelle esternalizzate, ricadono nello *scope* della funzione di revisione interna; - la funzione di revisione interna deve avere accesso a tutte le attività, comprese quelle esternalizzate, della banca, svolte sia presso gli uffici centrali sia presso le strutture periferiche. Il documento non affronta nel dettaglio le modalità di effettuazione dei controlli sulle attività esternalizzate, rimesse all'autonomia delle banche; rimane ferma la responsabilità dell'IA di effettuare i controlli di terzo livello nel rispetto dei principi sopra menzionati.
Sezione III (Funzioni aziendali di controllo), par. 3.5 (Rapporti tra le funzioni aziendali di controllo e	**Attribuzione di compiti di controllo mediante accordi di servizio** È stato chiesto di prevedere la formalizzazione	No	L'attribuzione dei compiti e delle responsabilità tra le varie funzioni è determinato dall'OFSS nel documento previsto dalla Sez II, par. 5 e non è modificabile da accordi interfunzionali. Nel rispet-

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
altre funzioni aziendali)	dell'attribuzione dei compiti e delle responsabilità anche mediante accordi di servizio.		to di detto documento, rimane ferma la possibilità per le funzioni di IA e *compliance* di definire accordi di servizio.
	Reciprocità flussi informativi È stato chiesto di rafforzare i flussi informativi esplicitando che questi siano reciproci: anche le altre funzioni di controllo devono informare l'IA sull'attività svolta e le criticità riscontrate.	Sì	Testo modificato.
	Ambiti di collaborazione tra funzioni Con riferimento al punto "*Fermo restando la reciproca indipendenza e rispettivi ruoli aziendali, le funzioni aziendali di controllo collaborano tra loro e con le altre funzioni (es. funzione legale, organizzazione, sicurezza informatica) allo scopo di sviluppare le proprie metodologie di controllo*", è stato chiesto di non far riferimento esclusivamente alla sicurezza informatica, bensì alla sicurezza in generale, eliminando dalla frase il termine "informatica".	Sì	Testo modificato.
Sezione IV (Esternalizzazione di funzioni aziendali), par. 1 (Principi generali e requisiti particolari)	**Esternalizzazione infragruppo** E' stato chiesto di tenere distinte e disciplinare in modo diverso l'esternalizzazione (accentramento) presso la capogruppo o altre entità del gruppo e l'esternalizzazione presso terzi.	Sì	Testo modificato.
	E' stato anche chiesto di equiparare all'accentramento di gruppo l'esternalizzazione presso entità facenti parte dello stesso *network* .	No	Un possibile ruolo del network in tale ambito sarà valutato in occasione dell'adeguamento della normativa nazionale al pacchetto CRD IV – CRR, che detta una disciplina specifica per i *network*

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
			delle banche cooperative.
	Definizione di esternalizzazione È stato chiesto di eliminare la disposizione che limita il novero dei soggetti presso cui esternalizzare le funzioni di controllo (banche, società di revisione e organismi associativi) e di definire i requisiti di professionalità, indipendenza e organizzazione di cui il fornitore di servizi deve esse provvisto per assumere l'incarico.	No	È stata mantenuta l'impostazione della norma, che trova giustificazione nella delicatezza dello svolgimento delle attività di controllo. In tal senso, l'affidamento di tali funzioni è consentito solo a soggetti che già istituzionalmente svolgono attività bancaria o attività di controllo sulle banche; inoltre, sono consentite forme di esternalizzazione verso organismi associativi, riconoscendo il ruolo di supporto di tali organismi verso le banche di minore dimensione.
	Funzioni operative importanti È stato chiesto di limitare il novero delle funzioni operative importanti a quelle che siano effettivamente "essenziali".	No	Si ritiene che la definizione di funzione operativa importante attualmente utilizzata ricomprenda le funzioni aziendali che necessitano di adeguate cautele quando non svolte all'interno della banca.
	Esternalizzazione in paesi UE ed extra UE È stato chiesto di prevedere un procedimento amministrativo solo per le esternalizzazioni extra UE. E' stato chiesto di limitare l'obbligo di informativa preventiva alle sole esternalizzazioni presso soggetti con sede in paesi extra UE.	No	L'esternalizzazione di funzioni aziendali di controllo incide in maniera rilevante sull'assetto organizzativo delle banche; si ritiene pertanto opportuno che tali scelte vengano comunicate in anticipo all'autorità di vigilanza indipendentemente dal paese in cui è insediato il fornitore di servizi. Inoltre, si rappresenta che l'apertura di un procedimento amministrativo di divieto è soltanto eventuale.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	Procedimento di divieto dell'esternalizzazione È stato chiesto di riconsiderare i termini complessivi per il procedimento di divieto.	No	I termini indicati risultano congrui rispetto all'attività da svolgere e comunque inferiori rispetto al termine generale previsto dal Provvedimento del 25 giugno 2008 in materia di procedimenti amministrativi.
	È stato chiesto di prevedere l'obbligo di motivazione del procedimento di divieto.	Chiarimento	L'obbligo di motivazione è imposto in via generale dall'articolo 3 della l. 241/1990 e relative modifiche.
	Impatto sulla continuità operativa È stato chiesto di inserire nella politica aziendale in materia di esternalizzazione la valutazione dell'impatto in termini di continuità operativa.	Sì	Testo modificato.
	Competenze per reinternalizzare attività E' stato criticato l'obbligo di mantenimento delle competenze per la reinternalizzazione delle attività, soprattutto per le banche di ridotte dimensioni. Ne deriverebbero costi troppo elevati che inficerebbero la convenienza del ricorso all'esternalizzazione. E' stato proposto di limitare l'obbligo al mantenimento delle conoscenze per affidare il servizio ad altro fornitore di servizi. E' stato chiesto di chiarire modalità e termini per l'eventuale reinternalizzazione delle attività.	No	La disciplina in materia di esternalizzazione prevede che la società trattenga le competenze necessarie per poter re-internalizzare le funzioni esternalizzate in caso di necessità. Si ritiene che il mantenimento di competenze essenziali concernenti l'attività esternalizzata sia necessario, non solo per consentire l'effettività dei controlli sul fornitore di servizi, ma anche per non arrecare pregiudizio all'operatività aziendale nei casi in cui sia necessaria una reinternalizzazione. In generale, la valutazione delle competenze ritenute effettivamente necessarie è, innanzitutto, rimessa all'intermediario stesso. A titolo esemplificativo, nel caso di esternalizzazione delle funzioni di controllo, le competenze da mantenere

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
			possono consistere nella conoscenza e capacità di utilizzo delle metriche usate per la valutazione dell'esposizione ai rischi o delle regole e procedure oggetto di verifica da parte della funzione di *compliance*.
	Accesso ai locali da parte dell'AdV È stato chiesto di chiarire la disposizione che impone di inserire nel contratto di esternalizzazione la previsione del diritto di accesso ai locali del fornitore di servizi da parte dell'AdV, non potendo questa ricorrere alla forza pubblica in caso di inadempimento.	Chiarimento	La violazione dell'obbligo contrattuale per il fornitore di servizi di consentire all'AdV l'accesso ai locali di quest'ultimo costituisce inadempimento contrattuale e pertanto dà titolo alla banca di richiedere l'adempimento o la risoluzione ai sensi dell'articolo 1453 c.c.
	Garanzia del livello di servizio In tema di contenuto del contratto di esternalizzazione è stato chiesto di chiarire se tra le clausole obbligatorie, relative agli eventi che potrebbero compromettere la capacità del fornitore di garantire il servizio, debbano essere inserite le *performance* finanziarie e i mutamenti importanti nella struttura organizzativa e proprietaria del fornitore.	Chiarimento	L'individuazione degli eventi che potrebbero compromettere la capacità del fornitore di garantire un livello di servizio adeguato è rimessa alla valutazione delle banche; le *performance* finanziarie e i mutamenti importanti nella struttura organizzativa e proprietaria del fornitore rientrano tra gli elementi rilevanti da prendere in considerazione.
	Clausole risolutive espresse Con riferimento alle clausole risolutive espresse che consentono alla banca di porre termine all'accordo di esternalizzazione "*quando si verifichi il mancato rispetto del livello di servizio concordato*", è stato chiesto di limitare tali clausole ai casi in cui ci sia un concreto e comprovato pregiudizio alla continuità del *business*. Si propone pertanto di modificare la disposizione come segue "*quando si verifichi un generalizzato, grave e*	No	È rimessa all'autonomia negoziale delle parti l'individuazione delle fattispecie in cui si ritiene non rispettato il livello di servizio concordato.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	continuo mancato rispetto del livello di servizio concordato e che esso sia acclarato dalle Funzioni competenti della banca".		
	Allineamento della terminologia È stato chiesto di utilizzare le locuzioni "piano di continuità operativa" e "procedure di continuità" in luogo rispettivamente di "piano di emergenza" e "procedure di emergenza", allineando i termini utilizzati a quanto previsto nel Capitolo 9 in materia di continuità operativa.	Si	Testo modificato.
	Controlli su funzioni operative importanti non di controllo esternalizzate Con riferimento alle funzioni operative importanti esternalizzate, è stato chiesto il riconoscimento di una maggiore flessibilità organizzativa nelle modalità di controllo su tali attività, specie con riguardo alla possibilità di non individuare un referente per le attività esternalizzate e di enfatizzare il ruolo del *network* delle banche di credito cooperativo.	No	Si ritiene che la presenza di un referente per i controlli sulle funzioni importanti esternalizzate sia necessaria per garantire l'effettività dei controlli sul fornitore di servizi. Un possibile ruolo del *network* in tale ambito sarà valutato in occasione dell'adeguamento della normativa nazionale al pacchetto CRD IV – CRR.
	Relazione annuale È stato chiesto di chiarire se la relazione annuale debba essere redatta dal referente per le attività esternalizzate competente a controllare le singole funzioni esternalizzate o dall'IA (o, nel caso di esternalizzazione di quest'ultima, dal referente dell'IA). In tale ultimo caso, è stato chiesto di chiarire se sia obbligatoria l'integrale copertura annuale di tutti gli ambiti esternalizzati o possa essere seguita una pianificazione *risk*	Chiarimento	La relazione sulle attività esternalizzate è redatta annualmente dall'IA, basandosi sia sull'attività di controllo svolta dal referente per le attività esternalizzate sia sugli accertamenti eventualmente svolti, in base al piano *audit*, dalla funzione di revisione interna. In generale la relazione annuale deve essere redatta dal referente della funzione di revisione in-

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	based. È stato altresì chiesto di precisare meglio l'ambito della relazione e di chiarire se questa possa essere parte integrante della relazione annuale svolta dall'IA. E' stato proposto che la relazione annuale sia redatta dal fornitore di servizi in coordinamento con il referente aziendale. A proposito della relazione annuale sui controlli svolti per le funzioni esternalizzate è stato chiesto per le BCC di consentire che tale relazione sia redatta dalla funzione di revisione interna esternalizzata alla Federazione di competenza delle BCC.		terna che, ferma restando la sua responsabilità, può avvalersi della collaborazione del fornitore di servizi. Con riferimento alle BCC, che esternalizzano l'IA presso la federazione di categoria, la relazione può essere redatta dalla funzione esternalizzata e verificata dal referente interno.
	Referenti E' stata proposta la possibilità di designare nelle realtà più complesse più di un referente per le attività esternalizzate.	Chiarimento	Nelle realtà più complesse è ammissibile la presenza di più referenti per le attività esternalizzate.
	Approvazione della relazione dell'IA È stato chiesto di limitare l'approvazione dell'OFSS alla parte di relazione dell'IA sulle attività esternalizzate relativa alle azioni correttive adottate e non a tutto il testo della relazione stessa, al fine di non compromettere l'autonomia di giudizio dell'IA.	No	Si ritiene che il responsabile ultimo del buon funzionamento delle attività esternalizzate sia l'OFSS, che pertanto fa propria, approvandola, la relazione dell'IA circa il corretto svolgimento, da parte del fornitore di servizi, delle attività esternalizzate.
	Azioni correttive È stato chiesto se per "*conseguenti misure correttive adottate*" si debbano intendere le azioni correttive richieste al fornitore e non ancora attuate oppure solo	Chiarimento	Devono essere indicate sia le azioni correttive già attuate, sia quelle solo richieste ma non ancora attuate.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	quelle già attuate.		
Sezione IV (Esternalizzazione di funzioni aziendali), par. 2 (Esternalizzazione del trattamento del contante)	**Utilizzo delle verifiche dell'IA di gruppo** È stato chiesto se nel caso in cui le attività di *audit* su processi in *outsourcing* vengano svolte dalla funzione di *audit* del gruppo, ma non direttamente dalla funzione *internal audit* locale, possano essere prese in considerazione le risultanze delle verifiche condotte dall'IA di gruppo ai fini della stesura della nuova relazione annuale sulle attività esternalizzate, anche se non incluse nel piano di *audit* locale.	Chiarimento	Si ritiene ammissibile l'utilizzo delle risultanze dei controlli dell'IA di gruppo nella relazione redatta dall'IA locale, ove rilevanti.
	Integrazione delle disposizioni E' stato suggerito di inserire nelle disposizioni sui controlli interni le previsioni di cui al Provvedimento del 14 febbraio 2012 in tema di disposizioni relative al controllo dell'autenticità e idoneità delle banconote in euro e al loro ricircolo, con specifico riferimento alle verifiche annuali di competenza della funzione di *internal audit* e di *compliance*, cogliendo l'occasione per un chiarimento degli ambiti di competenza.	Chiarimento	Nella valutazione delle attività concernenti l'esternalizzazione del trattamento del contante, sono coinvolte tutte le funzioni aziendali di controllo, secondo il riparto di competenze stabilito dalle presenti disposizioni (cfr. Sez. III).
	È stato proposto di riformulare la citata disposizioni rafforzando la posizione della banca, in particolare si suggerisce la seguente formulazione: "*il diritto per la banca di recedere, senza penalità, nel caso in cui la controparte violi uno qualunque degli obblighi di cui al contratto e non vi ponga rimedio entro il periodo di tempo indicato nel contratto stesso*".	Sì	Testo modificato.
	Elenco delle attività esternalizzabili	No	Le presenti disposizioni, tenuto conto della difficoltà di individuare in modo tassativo le attività

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	È stato chiesto di introdurre un elenco tassativo di attività esternalizzabili.		astrattamente esternalizzabili, adottano un approccio in base al quale, da un lato, indicano le attività che non possono essere esternalizzate e, dall'altro, prevedono le condizioni per esternalizzare le restanti attività. Si ritiene che tale approccio consenta di contemperare al meglio l'esigenza di flessibilità organizzativa delle banche con quella di presidiare adeguatamente i rischi del ricorso all'*outsourcing*.
	Funzione antiriciclaggio È stato chiesto di menzionare la funzione antiriciclaggio tra le funzioni aziendali di controllo atte al monitoraggio e alla valutazione delle procedure seguite per l'allacciamento e la gestione dei rapporti di esternalizzazione del trattamento del contante.	Chiarimento	Tra le funzioni aziendali di controllo rientra anche la funzione antiriciclaggio che, per gli aspetti di competenza, può essere coinvolta nella valutazione delle procedure seguite per l'allacciamento e la gestione dei rapporti di esternalizzazione del trattamento del contante.
Sezione V (Il sistema dei controlli interni nei gruppi)	**Esternalizzazione presso la capogruppo** È stato chiesto di semplificare le procedure per l'esternalizzazione delle funzioni aziendali di controllo presso la capogruppo.	Sì	Testo modificato.
	E' stato chiesto di chiarire modalità e meccanismi di funzionamento e di governo dell'audit su base consolidata.	Chiarimento	Ferma restando la responsabilità degli organi aziendali delle singole componenti del gruppo sull'adeguatezza, efficacia ed efficienza del sistema dei controlli interni a livello individuale, la capogruppo definisce le politiche e i principi di revisione interna per tutto il gruppo, incluse le metodologie e le misure per assicurare la qualità

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
			dei processi di *audit*.
	Esenzione dell'istituzione dell'IA per controllate È stato chiesto di valutare se 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 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 parte	La disciplina dell'esternalizzazione all'interno dei gruppi è stata complessivamente rivista. In tale ambito, è consentito l'accentramento delle funzioni aziendali di controllo, fermo restando la responsabilità degli organi aziendali delle controllate circa il buon funzionamento dei controlli interni.
Sezione V (Il sistema dei controlli interni nei gruppi), par. 2 (Controlli interni di gruppo)	**Riporto gerarchico referente** È stato chiesto di eliminare la previsione che impone la subordinazione gerarchica del referente presso la controllata alla funzione di controllo esternalizzata presso la capogruppo.	Si	Testo modificato.
	Accesso ai dati delle controllate È stato chiesto di consentire alle funzioni aziendali di controllo, al fine di svolgere in modo appropriato i propri compiti, di avere accesso anche ai dati di tutte le società controllate sia italiane, sia estere.	Chiarimento	La disponibilità dei dati concernenti le società controllate dovrebbe essere garantita dalla capogruppo nell'esercizio dei suoi poteri di direzione e coordinamento e in ottemperanza alla normativa applicabile.
	Ruolo del referente in esternalizzazione infragruppo È stato osservato che nel caso di affidamento in *service* delle funzioni di controllo alla capogruppo, la previ-	Sì	Testo modificato.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	sione della necessità di un referente "*incaricato della complessiva supervisione della specifica attività di controllo esternalizzata*" appare eccessiva e fuorviante nei meccanismi di relazione con la capogruppo. In tale ipotesi, il referente dovrebbe svolgere una funzione di supporto al fornitore di servizi piuttosto che un compito di controllo del rispetto dei livelli di servizio da parte del medesimo. È stata dunque proposta una riformulazione delle previsioni regolamentari in tal senso.		
	Referenti dell'IA e esternalizzazione infragruppo È stato evidenziato che alcune soluzioni organizzative ed operative che il Documento richiede con riferimento all'IA della capogruppo, nel caso di esternalizzazione dell'IA da parte delle società controllate, produrrebbero in generale diseconomie, ancor più per organizzazioni di minori dimensioni e con un ridotto numero di società controllate. In particolare è stato suggerito, nel caso di esternalizzazione delle funzioni di controllo presso la capogruppo, di prevedere la "possibilità" e non l'"obbligo" d'individuare degli appositi referenti interni a supporto dei fornitori di servizi o, in seconda istanza, di prevedere l'obbligo soltanto per banche e istituzioni finanziarie per cui è normativamente previsto il responsabile della funzione di revisione interna, escludendo pertanto le società di servizi e strumentali.	Chiarimento	Nel caso di esternalizzazione infragruppo l'individuazione di un referente è obbligatoria per le banche. Con riferimento alle altre entità, è rimessa alla valutazione della capogruppo l'opportunità di nominare un referente qualora l'entità in questione assuma rischi considerati rilevanti per il gruppo.
	Responsabilità direzione generale È stato chiesto di attribuire alla direzione generale della società controllata la responsabilità dei controlli sulla funzione di controllo accentrata presso la capogruppo.	In parte	La disciplina dell'esternalizzazione infragruppo è stata complessivamente rivista. In tale ambito, il referente della funzione di controllo esternalizzata presso la capogruppo non ha funzioni di controllo ma di supporto e può essere eventualmente

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
			individuato, nelle banche di minore dimensione e complessità, nella direzione generale della controllata.
	Riporto del referente verso il fornitore di servizi Viene prospettata l'opportunità di considerare anche il riporto manageriale/funzionale del referente verso la struttura della società che svolge il servizio in *outsourcing*.	No	Il referente è un punto di riferimento per la struttura che effettuerà i controlli. Tuttavia, questi non può che riportare agli organi aziendali della propria società. Naturalmente egli dovrà collaborare attivamente con il soggetto presso cui sono esternalizzate le funzioni di controllo.
	Referente È stato chiesto se i referenti all'interno delle controllate debbano essere dipendenti o possano essere soggetti designati dalla capogruppo.	Chiarimento	Le disposizioni non impongono che il referente sia un dipendente della banca che esternalizza le funzioni di controllo.
	Referente e responsabile È stato chiesto se il referente interno per la funzione di *compliance* esternalizzata debba essere il responsabile della relativa funzione. In caso di risposta negativa, è stato chiesto se il referente sia responsabile nei confronti degli organi aziendali e dell'AdV di eventuali carenze nell'attività di *compliance* svolta dal fornitore di servizi.	Chiarimento	Il referente per la funzione di controllo esternalizzata all'interno del gruppo svolge un ruolo di supporto per detta funzione, incardinata presso la società cui è stata esternalizzata. Il referente è responsabile per l'espletamento dei compiti che gli sono attribuiti dalle presenti disposizioni (es.: supporto alla funzione di controllo esternalizzata, segnalazione di eventi e situazioni particolari).
	IA di gruppo e IA individuale È stato chiesto di eliminare le previsione che impone, nei casi di esternalizzazione dell'IA presso la capogruppo, la separazione tra l'unità incaricata dell'IA di gruppo da quella incaricata dell'IA individuale.	Sì	Testo modificato.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	Oggetto della relazione annuale È stato chiesto di chiarire se la relazione che la capogruppo deve inviare annualmente alla Banca d'Italia debba avere a oggetto solo accertamenti effettuati in loco dall'IA di gruppo oppure tutti gli accertamenti effettuati sulle società controllate da tutte le funzioni di controllo.	Chiarimento	La relazione deve avere a oggetto tutti gli accertamenti effettuati sulle società controllate da parte di tutte le funzioni di controllo (il suo contenuto non è quindi limitato agli accertamenti in loco effettuati dall'IA).
	Esternalizzazione in un paese terzo È stato chiesto di chiarire se la Sezione IV (*Outsourcing*) si applica solo all'esternalizzazione di funzioni aziendali importanti o di controllo presso soggetti con sede in altri paesi.	Chiarimento	La disciplina dell'esternalizzazione si applica a tutte le fattispecie di *outsourcing* indipendentemente dal paese ove è insediato il fornitore. Nel caso di esternalizzazione al di fuori del gruppo bancario si applica la Sezione IV, nel caso di esternalizzazione all'interno del gruppo bancario si applica la Sezione V.
	Gruppi *cross border* È stato chiesto di applicare il principio di proporzionalità ai gruppi *cross border*, nel senso di ritenere sostanzialmente soddisfatti i requisiti imposti dalla normativa italiana quando la capogruppo rispetta i requisiti imposti dall'autorità home.	No	Le filiazioni di banche comunitarie sono tenute a rispettare la normativa dello Stato in cui sono insediate. Consentire l'applicazione di norme di altri paesi a soggetti italiani comporterebbe, oltre che difficoltà sul piano della verifica del rispetto della norma da parte dell'autorità di vigilanza e del relativo *enforcement*, un trattamento discriminatorio nei confronti di soggetti con capogruppo insediata in Italia.
	È stato chiesto di consentire alle filiazioni di banche comunitarie di adottare le politiche, le procedure e i controlli stabiliti a livello di gruppo.	Chiarimento	Le filiazioni delle banche comunitarie possono adottare le politiche, le procedure e i controlli stabiliti dalla capogruppo nei limiti in cui questi siano conformi alla normativa italiana.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	È stato proposto di eliminare la necessità per l'OFG di filiazioni di banche comunitarie di definire il processo di gestione del rischio, facendo riferimento a quello di gruppo.	No	L'OFG è libero di adottare il processo di gestione del rischio deliberato a livello di gruppo, se coerente con la disciplina nazionale. È, inoltre, necessario che ci sia un formale atto di adozione di tale processo al fine anche di responsabilizzare gli organi aziendali sull'adeguatezza del processo di gestione del rischio di gruppo rispetto alle peculiarità del contesto in cui la filiazione opera.
	Obblighi di comunicazione È stato chiesto di esentare dagli oneri di comunicazione le fattispecie di esternalizzazione infragruppo.	No	L'esternalizzazione di funzioni aziendali di controllo incide in maniera rilevante sull'assetto organizzativo delle banche, anche se appartenenti a un gruppo. Si ritiene pertanto opportuno che tali scelte vengano comunicate in anticipo all'autorità di vigilanza.
	Decisioni strategiche su strutture di gruppo E' stato chiesto di intendere per decisioni strategiche in merito all'utilizzo di strutture accentrate (da riservare all'organo con funzione di supervisione strategica), le sole decisioni riferite al modello di presidio di gruppo e non alle singole decisioni per ogni società del gruppo, cosa ritenuta eccessivamente onerosa.	Sì	Testo modificato.
	Esclusione delle società strumentali dal perimetro della disciplina E' stato proposto di applicare la disciplina del documento di consultazione solo al perimetro delle società bancarie del gruppo e non a quello delle società strumentali o di servizi.	No	Si ritiene che, ferma restando l'applicazione dei criteri di proporzionalità, l'ambito dei controlli deve coincidere con tutto il perimetro del gruppo, ivi incluse le società strumentali che, ad es., quando gestiscono il sistema informativo, possono essere fonti di rischi non irrilevanti per tutto il gruppo.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	Valutazione delle scelte di esternalizzazione E' stato chiesto di chiarire se la valutazione periodica, costi-benefici, sulle scelte di esternalizzazione/accentramento infragruppo sia di esclusiva spettanza della capogruppo e riguardi una valutazione integrata del gruppo nel suo complesso.	Chiarimento	La valutazione periodica dei costi, dei benefici e dei rischi deve essere condotta dalla capogruppo e riguardare il gruppo nel suo complesso.
Sezione VII (Procedure di allerta interna)			La Sezione relativa alle procedure di allerta interna è stata momentaneamente stralciata in attesa di modificare il TUB per recepire la direttiva CRD IV, che contiene specifiche disposizioni su tali profili. La disciplina sulle procedura di allerta interna verrà, pertanto, emanata nell'ambito del recepimento di detta direttiva.
Sezione VIII (Succursali di banche comunitarie e di banche extracomunitarie aventi sede nei paesi del G10 o in quelli inclusi in un elenco pubblicato dalla Banca d'Italia)	**Disposizioni applicabili** È stato chiesto se alle succursali di banche comunitarie si applichino anche altre previsioni del Capitolo VII relativo al Sistema dei controlli interni.	Chiarimento	Alle succursali di banche comunitarie o insediate in stati appartenenti al G-10 si applicano esclusivamente le specifiche disposizioni previste nella Sezione VIII.
	Contenuto dell'attestazione È stato chiesto di limitare le materie oggetto dell'attestazione circa la verifica della conformità della succursale alle norme ad essa applicabili a quelle sottoposte al controllo della Banca d'Italia.	No	Il rischio di *compliance* riguarda tutta la normativa cui la succursale è soggetta, non solo quella di matrice bancaria e finanziaria.
	È stato proposto di modificare la disposizione sul contenuto dell'attestazione, inserendo una descrizione: i) dell'attività svolta dalla succursale; ii) delle soluzioni	Sì	Testo modificato.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	organizzative adottate; iii) degli esiti delle verifiche effettuate nell'anno; iv) delle verifiche pianificate per l'anno successivo.		
	Verifiche di adeguatezza È stato chiesto di chiarire se le verifiche sull'adeguatezza delle procedure interne debbano essere effettuate dalla casa madre o dalla stessa succursale.	Chiarimento	La verifica dell'adeguatezza deve essere condotta dalla impresa madre europea (cfr. Circolare 263, Tit. I, Cap. 1, parte II, Sez. 2, par. 2).
	Legale rappresentante È stato chiesto di chiarire se il legale rappresentante sia quello della succursale o della banca.	Chiarimento	Le disposizioni fanno riferimento al legale rappresentante della succursale.
Sezione IX (Informativa alla Banca d'Italia)	**Relazione della funzione antiriciclaggio** È stato chiesto di prevedere relativamente alla trasmissione tempestiva alla Banca d'Italia delle relazioni sull'attività svolta redatte periodicamente dalle funzioni di controllo, anche le relazioni della funzione antiriciclaggio.	Chiarimento	La funzione antiriciclaggio, e i relativi oneri informativi, sono disciplinati nel provvedimento del 10 marzo 2011.
	Contenuto della relazione nel caso di gruppo È stato chiesto di prevedere che la relazione predisposta dalla capogruppo rappresenti anche una sintesi dei principali aspetti inerenti alle entità del gruppo senza l'obbligo di trasmissione di tutti i documenti per ciascuna entità. In alternativa è stato suggerito di prevedere una relazione *ad hoc* che sintetizzi i principali aspetti rilevati nei documenti delle entità o di limitare l'obbligo di trasmis-	Sì	Testo modificato.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	sione alle sole entità del gruppo aventi sede in Italia.		
Allegato A (Disposizioni speciali relative a particolari categorie di rischio)	**Rischio strategico** È stato chiesto di prevedere disposizioni specifiche per il rischio strategico.	Chiarimento	L'elenco contenuto nell'allegato A è meramente ricognitivo delle disposizioni organizzative speciali dettate con riferimento ai singoli rischi. Con riferimento al rischio strategico si applicano le disposizioni contenute nel Titolo III, Capitolo 1, in materia di processo di controllo prudenziale.
Allegato A (Disposizioni speciali relative a particolari categorie di rischio), par. 2 (Rischio di credito e di controparte) e 2.1 (Valutazione del merito di credito)	**Controlli effettuate da strutture diverse dalle funzioni di controllo** È stato chiesto di precisare entro quali limiti (ad es., in caso di assenza di poteri deliberativi significativi) e/o con quali modalità (ad es., definizione di dettaglio del perimetro di responsabilità e delle modalità di interrelazione con le funzioni di controllo) possano se del caso essere effettuati controlli di primo livello di seconda istanza e/o di secondo livello anche da parte di strutture organizzative solitamente non esercitanti le funzioni di controllo richiamate nel documento (ad es., controlli sulla filiera del credito effettuati da strutture creditizie).	In parte	Testo modificato. È demandato all'autonomia organizzativa della banca, nel rispetto dei principi generali della disciplina sui controlli interni, stabilire quali siano le strutture competenti a effettuare i controlli di primo livello, anche di seconda istanza. I compiti del RM (cfr. Sez. III, par. 3.3) non possono essere assegnati a funzioni competenti a effettuare i controlli di primo livello. Ciò posto, si ritiene che sia ammissibile l'assegnazione di controlli sulla filiera del credito (a titolo di esempio, il controllo andamentale e il monitoraggio delle singole posizioni) a strutture di primo livello, purché: a) questo non precluda al RM di svolgere i compiti ad esso attribuiti dalla normativa, tra cui il monitoraggio costante dell'evoluzione del rischio di credito e del rispetto dei limiti operativi; b) queste strutture di primo livello svolgano i controlli ad esse attribuiti nel rispetto dei principi stabiliti dalla normativa (cfr., in particolare, Sez. I, par. 6 "Principi generali"). In ogni caso, la verifica del corretto svolgimento

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
			del monitoraggio andamentale sulle singole esposizioni, in particolare di quelle deteriorate, e la valutazione della coerenza delle classificazioni, della congruità degli accantonamenti e dell'adeguatezza del processo di recupero è svolta, a livello centrale e periferico, dalla funzione di controllo dei rischi o, per le banche di maggiore dimensione e complessità operativa, da una specifica unità, che riporta al responsabile della funzione di controllo dei rischi.
	Valutazione del merito di credito Con riferimento alla valutazione del merito di credito, è stato chiesto di meglio articolare la previsione per portafogli e/o secondo il criterio di proporzionalità. In particolare, è stato chiesto che il requisito normativo in esame possa intendersi limitato alle controparti *corporate* e bancarie, non considerando necessaria, o eventualmente solo per le banche di maggiori dimensioni in applicazione del principio di proporzionalità, una valutazione anche del merito di credito delle controparti sovrane, per le quali tale valutazione sarebbe ulteriormente complessa.	Sì	Testo modificato.
	Verifiche periodiche È stato chiesto di chiarire se il compito di verifica periodica dell'intero processo di gestione del rischio di credito e di controparte sia da intendersi in carico alla funzione di *internal audit*.	Chiarimento	L'IA è coinvolta nella verifica del processo di gestione del rischio di credito in qualità di controllore di terzo livello. Il monitoraggio nel continuo spetta alla funzione di controllo dei rischi.
Allegato A (Disposizioni speciali relative a particolari categorie di	**Controparti centrali**	No	La disposizione è di derivazione comunitaria (cfr.

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
rischio), par. 4 (Concentrazione dei rischi)	Si chiede di eliminare nel testo la parte "incluse le controparti centrali".		art. 81 della CRD IV).
Allegato A (Disposizioni speciali relative a particolari categorie di rischio), par. 8 (Rischi operativi)	**Rischio informatico** È stato chiesto di menzionare anche il rischio informatico.	No	Si fa presente che, in generale, il rischio informatico rientra tra i rischi operativi. In considerazione della rilevanza di tale rischio, il Capitolo 8 (Sistema informativo) detta una disciplina specifica per la sua gestione.
Allegato A (Disposizioni speciali relative a particolari categorie di rischio), par. 10 (Rischio di leva finanziaria eccessiva)	**Leva finanziaria** È stato chiesto di non introdurre la previsione sulla leva finanziaria fino a quando non sia definita la normativa di riferimento.	No	La disposizione è di derivazione comunitaria (cfr. art. 87 della CRD IV).
Allegato B (Controlli sulle succursali estere)	**Definizione di operatività significativa** È stato chiesto di indicare a titolo esemplificativo criteri qualitativi e quantitativi sulla base dei quali declinare il concetto di '"operatività significativa". Al riguardo si ritiene possano rilevare: aspetti inerenti le autonomie deliberative, la tipologia dei prodotti commercializzati, la legislazione locale di riferimento.	Sì	Testo modificato.
	Periodicità delle verifiche È stato chiesto di non demandare all'OFG il compito di fissare la periodicità minima delle verifiche.	Sì	Testo modificato
	Ruolo di referente della *compliance* È stato chiesto se, nelle filiali caratterizzate da	Chiarimento	Nelle filiali non significative e caratterizzate da una limitata complessità operativa il ruolo di referente della *compliance* può essere attribuito, oltre

CAPITOLO 7 Il sistema dei controlli interni			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
	un'operatività non complessa, il ruolo di referente della *compliance* possa essere attribuito a un dipendente con ruoli operativi (*banker* o responsabile della succursale).		che a soggetti senza ruoli operativi o privi di conflitti di interessi con le attività oggetto di controllo, al responsabile della filiale.
	Modalità di riporto È stato suggerito di non definire in modo rigido la tipologia di riporto tra le funzioni locali di controllo e le funzioni centrali, salvo il principio condivisibile delle doppie linee di riporto (che constano nel riporto verso il dirigente preposto alla succursale e verso le strutture di controllo centrali).	Chiarimento	La formulazione della disposizione è sufficientemente flessibile, prevedendo "di norma" il riporto gerarchico alle funzioni di controllo centrali degli addetti all'unità di controllo della filiale. Le banche, dunque, possono, motivandone la ragione, discostarsi da tale previsione, fermo restando il doppio riporto informativo al responsabile locale e all'unità centrale.
	Verifiche sul reddito prodotto e sui rischi assunti In merito al compito di "*effettuare il controllo documentale su tutti gli aspetti dell'operatività ed estenderlo anche al merito della gestione in modo da condurre ad una valutazione complessiva dell'andamento delle succursali estere, sotto il profilo del reddito prodotto e dei rischi assunti*", è stato chiesto di precisare meglio quale funzione sia deputata allo svolgimento delle verifiche descritte e debba riferire sull'esito delle stesse all'OFSS.	Chiarimento	Le diverse funzioni competenti sulle varie tematiche devono effettuare i controlli il cui esito va sottoposto all'OFG, che riferisce annualmente all'OFSS.
	Inserimento sul mercato È stato chiesto di precisare quale rischio si intenda presidiare con la previsione che la funzione di revisione interna debba verificare *inter alia* l'inserimento sul mercato della succursale estera.	Chiarimento	La verifica dell'inserimento sul mercato è, tra l'altro, funzionale a valutare la coerenza dei risultati della succursale con gli indirizzi strategici e il *business model* della banca.

CAPITOLO 8 Sistema informativo

A. Risposte ai BOX

Box 4 - Interazioni tra rischio informatico e rischi operativi (Capitolo 8, Sezione II, par. 1)

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

Commenti e proposte

Sarebbe auspicabile che venisse esplicitamente richiamata l'opportunità di una stretta collaborazione tra l'*owner* del rischio informatico (non inquadrato come funzione di controllo di secondo livello e quindi non richiamato nel Capitolo 7, Sez. II, par. 5) e la funzione di *risk management/Operational risk management* (ORM); ad esempio, le attività di raccolta dati di perdita e le valutazioni di scenari di rischio sono spesso già svolte dalla funzione ORM anche con riferimento ai sistemi informativi.

È importante definire modalità strutturate per interagire con la funzione di *risk management*, al fine di integrare le valutazioni di carattere tecnologico nel più ampio processo di gestione e analisi del rischio operativo, così come metodologicamente definito da Basilea II e dalle prassi gestionali in campo ORM.
Lo sviluppo della modellistica/metodologia di analisi del rischio dovrebbe essere assegnato alla funzione indipendente del *risk management*.

Appare inoltre opportuno favorire l'introduzione di un modello di *reporting* sul rischio IT, condiviso tra le funzioni di *operational risk* e *IT security*, per la consuntivazione del rischio informatico, coerentemente con il modello di analisi dei rischi operativi, anche nell'ottica di migliorare l'esame e l'indirizzo delle strategie e del governo delle infrastrutture IT.

Valutazioni

Le proposte formulate sono, in linea generale, condivisibili. Si ritiene che – ferma restando la distinzione tra le attività di *risk management* che investono i sistemi informativi e quelle di analisi dei rischi informatici, in ordine agli obiettivi, alle procedure e strumenti utilizzati nonché alle competenze necessarie - sia opportuna una stretta collaborazione tra utente responsabile - che collabora all'analisi del rischio di uno specifico sistema di competenza, con l'obiettivo principale dell'individuazione dei presidi di sicurezza da applicare per ottenere un livello di rischio accettabile rispetto alle esigenze del *business* – e la funzione di *risk management*, che gestisce il rischio informatico con un'ottica di secondo livello. Inoltre, si condivide l'opportunità di integrare le metodologie dei *framework* adottati e di sfruttare le sinergie a livello operativo tra la funzione di *risk management* e il personale specialistico che collabora alle attività di analisi del rischio informatico.

Si ritiene, tuttavia, che la pratica bancaria e gli approfondimenti in sede accademica non consentano di fornire indicazioni normative di dettaglio sui modelli di valutazione e di reporting da adottare. Tali indicazioni potranno essere elaborate solo in presenza di un maggiore consolidamento delle esperienze in atto nel sistema bancario nonché degli standard di riferimento a livello internazionale.

Nella norma viene in ogni caso richiamata, tra i compiti dell'organo con funzioni di supervisione strategica, la necessità di garantire l'integrazione l'analisi del rischio informatico con i sistemi di misurazione e gestione dei rischi aziendali.

Box 5 – Controllo dei sistemi in *cloud computing* (Capitolo 8, Sezione VI, par. 3)

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

Commenti e proposte

In relazione alla valutazione dei rischi e delle opportunità delle applicazioni e dei dati che desiderano portare in *cloud* pubblico, si ravvisa la necessità di competenze multidisciplinari che riguardano, oltre agli aspetti concernenti il processo aziendale da automatizzare, l'architettura dei sistemi informativi e la sicurezza informatica, anche il profilo legale. Laddove, infatti, il fornitore sia caratterizzato da una gestione dell'infrastruttura tecnologica e dei data center non limitata ai confini nazionali rileva la necessità di contrattualizzare norme e leggi di riferimento a con riguardo ai propri obblighi di *compliance* (ad es., *privacy*, foro competente).

Con particolare riferimento al *cloud* pubblico, si sottolinea la rilevanza delle azioni messe in campo dal fornitore per isolare o segregare gli ambienti, le applicazioni e i dati della banca rispetto alla gestione di altri clienti.

Valutazioni

Le osservazioni formulate sono condivise. Per il caso di *cloud in community* o pubblico, è stata evidenziata: da una parte, l'eventualità che sia necessario predisporre controlli più complessi; dall'altra la valenza delle misure di isolamento degli ambienti dedicati a diversi utenti nell'ottica di attenuare i rischi di attacchi dall'interno e dall'esterno, così come di garantire il rispetto dei livelli di disponibilità di servizio concordati, anche in casi di emergenza o contesa di risorse.

B. Commenti alle disposizioni

CAPITOLO 8 Sistema informativo

CAPITOLO 8 Sistema informativo			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
Sezione I (Disposizioni di carattere generale), par. 1 (Premessa) e par. 2 (Fonti normative)	**Rapporto tra le disposizioni di Vigilanza e gli standard internazionali in materia di ICT** È stato osservato che le disposizioni dovrebbero focalizzarsi su indirizzi strategici (quali quelli contenuti nel par. 1 *" .. gli intermediari fanno riferimento agli standard e best practices …")* e su contenuti indispensabili per una consapevole assunzione dei rischi (cfr. Sez. III, approvazione del rischio residuo), senza richiamare nella normativa componenti anche importanti delle citate *best practices* che dovrebbero trovare una declinazione basata sul generale principio di proporzionalità e di "*capability level*" organizzativo. In proposito, è stato sottolineato che l'estrapolazione dal contesto di alcune parti delle *best practices* citate nel documento (COBIT, ITIL, ISO/IEC 27002:2005 – cfr. par. 2) potrebbe ingenerare dubbi interpretativi e difformità di applicazione che ne potrebbero limitare l'efficacia: nella definizione, pertanto, sarebbe preferibile fare riferimento al complessivo sistema di standard e delegarne l'applicazione secondo i criteri summenzionati. Il cambiamento degli standard nel corso degli ultimi anni (il passaggio dai British Standard agli ISO standard) potrebbe inoltre rendere non attuale e non coerente con lo standard in vigore le parti estrapolate ed inserite nella normativa. La lista degli standard inserita alla Sez. I, par. 2 non	Sì	Testo modificato. Gli standard internazionali sono intesi come strumento utile, in generale, per l'individuazione di adeguate misure per la gestione dei sistemi informativi, ma la loro adozione non rappresenta garanzia di *compliance* con la normativa di vigilanza. In altri termini, gli standard possono essere utilizzati come ausilio e complemento, fermo restando che le presenti disposizioni rappresentano requisiti minimi da rispettare. In questa ottica, al fine di evitare dubbi interpretativi, da un lato, viene eliminato l'elenco di standard (cfr. Sez. I, par. 2), e, dall'altro, si menziona la possibilità per gli intermediari di utilizzare standard e *best practices* in materia di ICT al fine di definire le concrete misure da adottare (cfr. ultimo periodo del par. 1).

CAPITOLO 8 Sistema informativo			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	dovrebbe essere considerata esaustiva, mentre dovrebbe essere rafforzata la generale valenza del principio circa l'opportunità di fare "*riferimento agli standard e best practices definiti a livello internazionale*".		
Sezione I (Disposizioni di carattere generale), par. 3 (Definizioni)	**Definizione di "incidente di sicurezza"** È stato osservato che appare opportuno inserire, fra le definizioni presenti nel paragrafo, anche quella di *"incidente di sicurezza*", inclusa nel successivo paragrafo "La gestione degli incidenti di sicurezza", 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)…*".	Sì	Testo modificato.
Sezione I (Disposizioni di carattere generale)	**Inventario risorse hardware e software** È stato osservato che è indispensabile, per una corretta valutazione della situazione ICT, prevedere la realizzazione di un Progetto/Mappa di Rete per l'infrastruttura esistente, o in fase di realizzazione, all'interno dell'intermediario. Il progetto di Rete è indispensabile per valutare correttamente i punti strategici di collegamento e di vulnerabilità dell'infrastruttura ICT. Esso ha anche la funzione di permettere un più rapido e corretto inventario degli strumenti hardware e software.	In parte	Testo modificato. Nella disciplina della gestione dei cambiamenti (Sez. IV) viene chiesto di predisporre e tenere costantemente aggiornato un inventario o mappa del patrimonio ICT (hardware, software, dati, procedure), funzionale anche alle attività di analisi e gestione del rischio informatico.

CAPITOLO 8 Sistema informativo			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
Sezione II (Governo e organizzazione dell'ICT), parr. 1 (Compiti dell'organo con funzione di supervisione strategica) e 2 (Compiti dell'organo con funzione di gestione)	**Competenze OFSS e OFG** È stato chiesto di riformulare e ridistribuire tra l'OFSS e l'OFG le competenze in materia di i) linee di indirizzo in materia di approvvigionamento delle risorse e ii) strumenti e modalità organizzative per lo sviluppo, la condivisione e aggiornamento di conoscenze in materia ICT.	In parte	Testo modificato. All'OFSS sono rimessi, in relazione alla loro valenza strategica, i compiti di: - approvazione delle linee di indirizzo in materia di approvvigionamento delle risorse: modalità di selezione del personale con funzioni tecniche e di acquisizione di sistemi, software e servizi, incluso il ricorso a fornitori esterni; - promozione dello sviluppo, della condivisione e dell'aggiornamento di conoscenze in materia di ICT all'interno dell'azienda. All'OFG, oltre alla definizione e attuazione della politica aziendale in materia di *outsourcing* (cfr. Capitolo VII, Sez. II, par. 3), è assegnato il compito di individuare gli strumenti e le modalità organizzative atte a garantire una gestione delle conoscenze in materia di ICT, in linea con gli obiettivi e gli indirizzi strategici aziendali.
	Documenti approvati dagli organi aziendali Al fine di applicare il principio di proporzionalità, è stato segnalato che l'interazione tra la banca e il fornitore di servizi – in merito alla definizione dell'architettura dei sistemi informativi, delle policy di sicurezza, delle metodologie per l'analisi del rischio informatico – può sottendere differenti modalità di generazione dei documenti sottoposti all'approvazione degli organi aziendali.	Sì	Testo modificato.

CAPITOLO 8 Sistema informativo			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	Competenze tecnico–manageriali dell'OFG È stato osservato che, nei contesti di tipo tradizionale in generale, e delle piccole banche in particolare, è problematica l'applicazione della norma secondo cui l'OFG ***"****… 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*.	Sì	Testo modificato. E' stato precisato che il requisito delle competenze si applica in via proporzionale alla complessità del contesto da gestire.
	Compiti dell'OFG Sono state proposte le seguenti modifiche: ***"[l'organo con funzione di gestione] approva*** ~~*disegna e segue*~~ *l'implementazione dei processi di gestione dell'ICT – incluso in particolare il processo di analisi del rischio informatico –* ***e ne monitora l'implementazione****, garantendo l'efficacia ed efficienza dell'impianto nonché la sua completezza e coerenza complessiva, con particolare riguardo ad una chiara e funzionale assegnazione di compiti e responsabilità, alla validità del supporto metodologico e procedurale;"*.	Sì	Testo modificato.
	Compiti dell'OFG – caso del *full outsourcing* È stata rilevata la necessità di una modulazione di alcuni compiti dell'OFG nei casi di *full outsourcing*, quali ad esempio: i) la definizione della struttura organizzativa della funzione ICT; ii) l'assegnazione di compiti e responsabilità all'interno della funzione ICT.	Sì	Testo modificato.
Sezione II (Governo e organizzazione dell'ICT), par.3 (Organizza-	**Organo responsabile dei sistemi informativi** Riguardo alla disciplina del "Direttore dei sistemi informativi o equivalente", è stato osservato che appare ec-	Sì	Testo modificato. La previsione è volta ad agevolare una gestione strategica, oltre che operativa, dei sistemi infor-

CAPITOLO 8 Sistema informativo			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
zione della funzione ICT)	cessivamente vincolante, rispetto alle autonome scelte organizzative, la previsione di un riporto gerarchico diretto di tale figura verso l'organo con funzione di gestione.		mativi, in linea con i principi della ICT *governance* e con le esigenze di flessibilità organizzativa delle banche. In tal senso, è previsto che esistano flussi informativi e linee di riporto funzionale tra la funzione ICT e l'organo con funzione di gestione.
	Organo responsabile dei sistemi informativi – caso della società strumentale di gruppo Nel caso di ICT in *outsourcing* interno al gruppo bancario, si ritiene il ruolo di direttore dei sistemi informativi sia attribuito al direttore generale della società interna di servizi, come figura responsabile *super partes* che riconduce ad unitarieta' le diverse componenti dei sistemi informativi del gruppo e che risponde direttamente all'organo di amministrazione e controllo della stessa ed indirettamente al consiglio di gestione della capogruppo, per il tramite della figura interna alla capogruppo di *chief operating officer*.	Chiarimento	E' ammessa l'assegnazione della responsabilità dei sistemi informativi al direttore generale della società di servizi ICT interna al gruppo, purché sia stabilito un canale di comunicazione diretto con l'organo con funzione di gestione della capogruppo.
	Compiti specialistici di analisi del rischio informatico Ferma restando la finalità di "*garantire l'indipendenza di giudizio*" e di "*utilizzare per il compito personale con adeguate caratteristiche professionali*", è stato chiesto di 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.	In parte	Testo modificato. Nelle realtà più complesse, l'indipendenza di giudizio rispetto alle funzioni operative del personale adibito ai compiti specialistici di analisi del rischio è garantita da un'adeguata collocazione organizzativa.

CAPITOLO 8 Sistema informativo			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	Comitati utente E' stato chiesto di prevedere l'obbligo per il fornitore di servizi di istituire, nella propria struttura, appositi comitati tecnici o simili, ai quali consentire la partecipazione dei clienti per condividere le scelte tecnologiche e per raccoglierne sistematicamente le esigenze. Il comitato avrebbe anche funzioni di controllo sul processo di adeguamento delle applicazioni, soprattutto ove scaturiscano da modificazioni normative di vigilanza o di legge.	In parte	Testo modificato. Non è previsto l'obbligo di istituire comitati utente ma, laddove presenti, è prevista la possibilità per l'intermediario di utilizzare tali comitati, da regolamentare nel contratto con il fornitore di servizi.
Sezione III (La gestione del rischio informatico)	**Comitati utente – analisi del rischio informatico** Nel caso delle realtà in *full outsourcing*, è stato chiesto di prevedere che la gestione del rischio informatico possa essere svolta sulla base di analisi tecniche condotte nell'ambito di comitati utente allo scopo costituiti presso il fornitore di servizi.	Sì	Testo modificato.
	Ruolo della funzione di controllo dei rischi E' stato richiesto un chiarimento in merito all'attribuzione formale dei compiti di analisi del rischio informatico, con riguardo in particolare al ruolo delle funzioni aziendali di controllo. Nello specifico è stato domandato se è possibile assegnare alle stesse la responsabilità dell'analisi, tenendo conto della necessità di *skills* altamente specialistici.	In parte	Testo modificato. Nella Sez. II è stato inserito un paragrafo sui compiti della funzione di controllo dei rischi. L'attività di analisi del rischio disciplinata alla Sez. III è tesa principalmente ad assicurare, per ciascun componente del sistema, l'individuazione dei presidi di sicurezza sufficienti a garantire un livello di rischio residuo contenuto e coerente con la propensione al rischio definita a livello aziendale. Per la sua rilevanza operativa, tale attività è svolta con il concorso dell'utente responsabile, del personale della funzione ICT, delle funzioni di controllo dei rischi, di sicurezza informatica e, ove ritenuto opportuno, dell'*audit*, secondo meto-

CAPITOLO 8 Sistema informativo			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
			dologie e responsabilità formalmente definite dall'organo con funzione di gestione.
	Rischio informatico potenziale In merito al rischio potenziale, è stato osservato come sia eccessivamente dispendioso e di utilità non chiara, doverlo valutare "*prima dell'applicazione degli opportuni presidi di sicurezza*", qualora questo significhi valutare il rischio al lordo di azioni mitiganti già in essere, ovvero valutare una situazione che di fatto non è quella reale.	In parte	Il rischio potenziale va valutato al lordo dei presidi in essere (nel caso di sistemi già in esercizio) e al netto degli eventuali presidi individuati nell'analisi dei rischi. Per evitare ambiguità, la frase menzionata ("*prima dell'applicazione degli opportuni presidi di sicurezza*") è stata eliminata.
	Ruolo del personale tecnico E' stata richiesta maggiore chiarezza con riguardo al processo di analisi e gestione del rischio informatico: la proposta normativa sembra avallare l'impostazione che inquadra nell'"utente responsabile" la figura di riferimento cui delegare tale attività, senza dare la giusta evidenza alla funzione di sicurezza informatica, oggi presente nell'assoluta maggioranza delle banche.	Sì	Testo modificato. La funzione di sicurezza informatica è stata inserita tra le funzioni aziendali che concorrono al processo di analisi del rischio.
	Registro degli incidenti di sicurezza Fra gli avvenimenti da documentare, previsti per la gestione del rischio informatico, è stato suggerito di introdurre quelli relativi agli incidenti per la sicurezza; quindi l'introduzione di un registro che dovrebbe contemplare: data, ora, utente che rileva il problema, descrizione, categoria (segnalazione antivirus, anomalia, perdita di un dato, presenza di *phishing* in posta elettronica, ecc.).	In parte	Testo modificato. Le disposizioni (cfr. Sez. IV, par. 6) sono state integrate prevedendo che le "*informazioni salienti dell'evento e i passi seguiti nella gestione dello stesso sono documentati*"**.**

CAPITOLO 8 Sistema informativo			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	Utente responsabile È stato chiesto di chiarire, al fine di evitare incertezze applicative della disciplina, la natura della nuova figura di utente responsabile identificata dalla normativa e che sembrerebbe essere riconducibile ad un ruolo di *system owner*. Tale "system owner" è definito dalla disciplina come "*la figura aziendale identificata per ciascun sistema che ne assume la generale responsabilità amministrativa in rappresentanza degli utenti, in rapporto con le funzioni preposte allo sviluppo e alla gestione tecnica*" e sembrerebbe corrispondere alla figura aziendale preposta alla certificazione del dato trattato informaticamente dalla procedura di riferimento e quindi esterna alla struttura di sviluppo ICT e più vicino ad una figura di *business/control owner* funzionalmente competente, che per molte realtà, soprattutto in Italia, sarebbe da identificare.	Chiarimento	L'utente responsabile è definito come la figura aziendale identificata per ciascun sistema o applicazione e che ne assume formalmente la responsabilità, in rappresentanza degli utenti e nei rapporti con le funzioni preposte allo sviluppo e alla gestione tecnica.

CAPITOLO 8 Sistema informativo			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	Utente responsabile – possibili inconvenienti È stato rilevato che l'attribuzione della responsabilità di eseguire l'analisi del rischio all'utente responsabile, 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 a un "utente", cioè a una figura di natura amministrativa, in quanto sistemi di infrastruttura (apparati di telecomunicazione, elaboratori centrali, ecc.); - rischi informatici non associabili a sistemi (applicazioni o infrastrutture), ma a processi (ad es., il processo gestione delle modifiche all'infrastruttura o alle applicazioni) che, seppur oggetto delle prescrizioni di cui alla Sez. IV "Il sistema di gestione della sicurezza informatica", dovrebbero comunque rientrare nell'ambito della valutazione del rischio.	Chiarimento	Si ritiene che i casi posti vadano risolti a livello aziendale, con opportune misure organizzative e metodologiche, in modo da garantire il rispetto dei requisiti posti dalla norma.
	Rischio residuo – ruolo dell'OFG In relazione alla previsione secondo cui *"… in ogni caso deve essere determinato il rischio residuo da sottoporre ad accettazione formale dell'utente responsabile …"* (par. 2, alinea 2), è stato chiesto di esplicitare che, qualora il livello di rischio residuo ecceda i limiti previsti per l'accettabilità da parte dell'utente responsabile, le misure di trattamento del rischio siano sottoposte	Sì	Testo modificato.

CAPITOLO 8 Sistema informativo			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	all'attenzione dell'organo con funzioni di gestione.		
Sezione IV (La gestione della sicurezza informatica), par. 3 (La sicurezza delle informazioni delle risorse ICT)	**Codice della "privacy"** È stato fatto presente che la regolamentazione dell'accesso logico ai sistemi deve assicurare al titolare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato tale da rendere indispensabile e indifferibile intervenire per necessità di operatività e di sicurezza del sistema (cfr. punto 10, Allegato B del d.lgs. 196/2003 – Codice in materia di protezione dei dati personali). Tenuto conto che sono disponibili tecniche di accesso al sistema tramite azzeramento della password dell'incaricato, ovvero attraverso la custodia delle password da parte del relativo custode, è necessario che le procedure di accesso ai dati e di controllo degli accessi siano descritte in questo contesto.	In parte	Testo modificato. La presente normativa in materia di sistemi informativi si applica senza pregiudizio per le disposizioni del Codice in materia di protezione dei dati personali (espressamente citato alla nota 12). Nello stabilire il requisito della riservatezza delle credenziali di autenticazione e della loro consegna nella disponibilità esclusiva dell'utente assegnatario, è fatta salva la possibilità di definire procedure sicure per permettere all'intermediario di accedere a dati aziendali in caso di necessità, in assenza degli utenti abilitati.
	Periodo di conservazione delle tracce elettroniche Con riguardo alla previsione relativa alla registrazione e conservazione delle tracce elettroniche relative alle operazioni critiche, si è ravvisata l'esigenza di un chiarimento in merito al rapporto con il Provvedimento del Garante per la protezione dei dati personali del 12 maggio 2011 in materia di circolazione delle informazioni bancarie e tracciamento delle operazioni bancarie. In particolare è stato chiesto di allineare l'ambito di applicazione, il contenuto dei log e i tempi di conservazione.	In parte	Testo modificato. E' stato uniformato il periodo di conservazione delle tracce, portandolo a 24 mesi, nell'ottica di semplificare la gestione e ridurre i costi. Non si ritiene, invece, di allineare al Provvedimento del Garante l'ambito delle operazioni tracciate, in quanto la previsione in discorso non ha l'obiettivo di garantire il rispetto della *privacy* dei clienti, ma quello di consentire la verifica di operazioni che potrebbero portare a frodi o altri incidenti di sicurezza.

CAPITOLO 8 Sistema informativo			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	Separazione degli ambienti di sviluppo, collaudo e produzione Premessa la condivisione del principio di separatezza fra ambienti di sviluppo e produzione, è stata segnalata 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.	Sì	Testo modificato.
	Sviluppo del software sicuro È stato chiesto di valutare l'opportunità di dettagliare meglio la "continuità operativa" anche come qualità di scrittura del software, quale componente strategica per la stabilità dei servizi di "*application management*".	In parte	Testo modificato Il punto riguarda solo marginalmente la continuità operativa e viene più propriamente trattato in questo capitolo, piuttosto che nel Capitolo 9 (La continuità operativa). In proposito, è stato inserito un requisito sull'adozione di metodologie e tecniche per lo sviluppo sicuro del software, quale possibile presidio di sicurezza da adottare sulla base dei risultati dell'analisi del rischio informatico.
Sezione V (Il sistema di gestione dei dati)	**Funzioni convolte nella *data governance*** È stato chiesto di precisare la disposizione 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*".	In parte	Testo modificato. La nota, riferendosi a figure "aziendali", cui necessitano competenze specifiche sulle informazioni trattate, contribuisce a chiarire come il contesto non sia confinato alla struttura tecnica.

CAPITOLO 8 Sistema informativo			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	Qualità e rilevanza dei dati È stato chiesto di precisare ed integrare il contenuto minimo dello standard aziendale di *data governance*, prevedendo che tale documento *«individua ruoli e responsabilità delle funzioni coinvolte nel trattamento (acquisizione, elaborazione, validazione ed utilizzo) dei dati, classifica i dati, sia operativi che gestionali, in funzione della loro rilevanza nel sistema informativo aziendale, identifica, in funzione della rilevanza, le misure atte a garantirne la qualità (in termini di completezza e accuratezza)».*	In parte	Testo modificato. Si è previsto che lo standard di *data governance*, pur senza fare riferimento a una classificazione dei dati in relazione alle esigenze di qualità (che andrebbe a sovrapporsi a quella di sicurezza), individui le misure da applicare per garantire la qualità delle informazioni trattate tenendo conto della loro rilevanza nel sistema informativo aziendale.
	Compiti dei responsabili della qualità dei dati Con riferimento alla previsione contenuta nella nota n. 25, relativa ai responsabili della qualità dei dati rilevanti, è stata fatta presente l'utilità di un maggior dettaglio del contenuto, anche in relazione alle responsabilità organizzative ad oggi in essere. In particolare i dati "*rilevanti*" di cui trattasi (informazione al mercato, segnalazioni all'OdV, valutazione dei rischi) sono di norma il risultato di un processo di elaborazione, validazione e controllo che coinvolge diversi attori, con responsabilità articolate e fissate dalla normativa di riferimento. L'obbligo, per le banche appartenenti alle macro-categorie 1 e 2, di individuare uno o più responsabili della qualità dei dati "rilevanti", pertanto, potrebbe apparire ridondante rispetto all'obbligo di "*definire ruoli e responsabilità delle funzioni coinvolte nel trattamento*" dei dati. Al contrario, potrebbe essere più utile prevedere che, per alcuni dati "rilevanti", sia stabilita una responsabilità in termini di validazione della qualità, consistente nella attestazione di avere ese-	Sì	Testo modificato.

CAPITOLO 8 Sistema informativo			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	guito tutti i controlli previsti (in termini di completezza e accuratezza) prima di rendere disponibili i dati ai fini della informativa "rilevante".		
	Controlli automatizzati È stato suggerito, almeno per i controlli chiave di processi critici, l'utilizzo di uno *standard* aziendale di *governance* dei controlli automatizzati (del tipo di quello utilizzato per i dati) che includa le politiche di documentazione e gestione del controllo e il riferimento al relativo rischio informatico.	In parte	Testo modificato. È stato inserito un riferimento alle procedure di controllo, che tratta della documentazione delle procedure di trattamento dei dati.
	Perimetro di applicazione La disposizione relativa al "*sistema di gestione dati*" prevede livelli omogenei di pervasività, strutturazione e completezza, la cui attuazione comporterebbe, per l'intermediario, investimenti e costi assai rilevanti (infatti, per qualunque dato gestito dovrebbero essere identificate e documentate le responsabilità, le procedure di gestione, estrazione ed elaborazione, le assunzioni e i criteri, i destinatari, ecc.). In relazione a ciò, è stato chiesto che siano applicabili criteri di rilevanza, di importanza, di progressività e di rischiosità, in modo da orientare strategicamente gli investimenti e costi connessi.	In parte	Testo modificato. E' stato introdotto il concetto di rilevanza delle informazioni nel sistema informativo (cfr. commento Qualità e rilevanza dei dati sopra). Inoltre, nel definire il "sistema di gestione dei dati", l'intermediario potrà censire i sistemi che conservano e trattano "informazioni aziendali", escludendo, ad es., strumenti di comunicazione informale interni.
Sezione V (Il sistema di gestione dei dati) (cfr. anche Capitolo 9 - Continuità operativa)	È stato suggerito di prevedere nei contratti con i fornitori di sistemi e servizi ICT requisiti di *disaster recovery* e di continuità operativa dei servizi e infrastrutture ICT oggetto di fornitura.	Chiarimento	La disposizione suggerita è già contenuta nella disciplina in materia di esternalizzazione del Capitolo 7, Sez. IV, applicabile anche all'esternalizzazione dei Servizi ICT.

CAPITOLO 8 Sistema informativo			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
Sezione VI (L'esternalizzazione del sistema informativo)	**Controllo delle funzioni esternalizzate** È stato suggerito di enfatizzare l'intervento delle funzioni aziendali di controllo nel monitoraggio dei rapporti con il fornitore e nello svolgimento di verifiche specifiche di *compliance* e di *internal audit* nel corso dell'intera durata del rapporto contrattuale, mirate a verificare il rispetto delle *policy* aziendali preventivamente definite e condivise con il fornitore di servizi.	Chiarimento	La disciplina sull'esternalizzazione del Capitolo 7, Sez. IV, applicabile anche all'esternalizzazione dei servizi ICT, richiede espressamente alla banca di controllare le funzioni esternalizzate.
	Società strumentali di gruppo È stato chiesto di specificare che, nel caso di affidamento di sistemi e servizi ICT a società strumentali di gruppo, non si applicano le disposizioni in particolare legate al contenimento del grado di dipendenza dal soggetto cui sono affidati i sistemi (in virtù della sua appartenenza al gruppo bancario), il mantenimento presso le singole banche delle competenze e la previsione di *exit strategies*.	Sì	Testo modificato.
	Rapporto di *outsourcing* vincolante È stato chiesto di non applicare le misure per evitare il *vendor lock in* ai contratti di *full outsourcing*, limitando tale previsione ad alcune componenti strumentali che effettivamente hanno la natura di fungibilità tra di loro.	No	In generale, oltre all'*outsourcing* di singole procedure o settori dei sistemi informativi, anche il *full outsourcing* è soggetto, a maggior ragione, al rischio di *vendor lock in*.
	Copia di backup È stata suggerita 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 back-up del proprio patrimonio informatico"*.	Sì	Testo modificato.

CAPITOLO 8 Sistema informativo			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	Messa a disposizione dei backup È stato chiesto di chiarire la necessità di confermare cosa si intenda per "*messa a disposizione"[delle copie di backup]*, evidenziando l'impraticabilità della consegna delle copie di *backup* qualora sia inclusa tra gli adempimenti.	Chiarimento	Si fa presente che tali copie possono essere rese disponibili attraverso un canale sicuro di rete (di adeguata capacità) ovvero in una locazione fisica concordata. In ogni caso, è prevista la possibilità per l'intermediario di accedere alle copie su richiesta.
	Cancellazione sicura dei dati È stato rilevato che, oltre all'onerosità, un'operazione di distruzione selettiva di parte del contenuto su backup si sostanzierebbe in un'alterazione della copia stessa, che non potrebbe più definirsi come l'immagine di quanto esistente nei sistemi di produzione alla data della copia originaria.	Chiarimento	Si osserva che il fornitore di servizi dispone di vari meccanismi e modalità per effettuare i *backup*. Si sottolinea, inoltre, che la prescrizione si applica solo a dati classificati come riservati.
Sezione VI (L'esternalizzazione del sistema informativo), par. 3 (Indicazioni particolari)	***Cloud computing* - definizione** È stato rilevato che la definizione di *cloud computing* ("*fruizione delle risorse informatiche nella forma di servizi accessibili via rete e configurabili in modo flessibile*") 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.	Sì	Testo modificato.
	Identificazione dei servizi in *cloud* È stato rilevato che sono in uso diversi servizi di tipo *cloud computing*, anche se non dichiarati come tali: molti dei servizi *smartphone*, i salvataggi di dati (foto, documenti) su dischi virtuali o spazi di memorizzazione dati messi a disposizione degli utenti dai fornitori dei	Chiarimento	Si assume che – così come esplicitamente richiesto in generale per qualsiasi iniziativa di esternalizzazione nel Capitolo VII - l'intermediario possegga tutte le competenze necessarie per vagliare l'opportunità e la conformità alle norme vigenti di soluzioni ICT gestite all'esterno, al di là

CAPITOLO 8 Sistema informativo			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	servizi internet, anche il servizio gmail. In questi casi il cliente (che è il titolare del trattamento ai sensi della normativa sulla *privacy*) non ha informazioni relativamente alla sicurezza, alla conservazione dei dati, sugli eventuali accessi da parte di altri, ecc. Inoltre le attività si svolgono sulla base dell'adesione del cliente/titolare del trattamento ai servizi forniti da un'entità non ben individuata, adesione del tipo "prendere o lasciare" che non da alcun diritto di verifica delle misure di sicurezza, non fornisce informazioni sulla modalità di conservazione e cancellazione dei dati.		della loro denominazione o presentazione commerciale.
Allegato B (Misure in materia di servizi telematici per la clientela) - eliminato	**Recepimento della normativa BCE sulla sicurezza dei pagamenti su internet** Al fine di facilitare l'implementazione delle misure richieste, risulterebbe utile procedere ad una omogeneizzazione organica dei requisiti o, in questa sede, limitarsi ad un richiamo alle normative esistenti (scelta adottata, ad esempio, nel Provvedimento di attuazione PSD: "*i prestatori di servizi di pagamento si attengono ai requisiti di sicurezza definiti nell'ambito dell'Eurosistema con riferimento agli strumenti di pagamento offerti alla clientela finale*").	Sì	L'allegato è stato eliminato; la normativa BCE è richiamata tra le fonti normative e pienamente operativa nell'ordinamento nazionale.

CAPITOLO 9 La continuità operativa

CAPITOLO 9 La continuità operativa			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	È stato chiesto di mantenere nelle nuove disposizioni il riferimento agli "standard definiti nell'ambito degli organismi di Categoria", che ha permesso alle banche di credito cooperativo di portare a fattore comune una serie di attività (ad esempio la *Business Impact Analisys*, la definizione di politiche strategiche, la formalizzazione del piano di continuità e delle modalità dei test). (Federcasse)	Chiarimento	Il testo in consultazione riproduce nella sostanza la disciplina vigente e non preclude la cooperazione in ambiti associativi per definire standard comuni, ferma restando la responsabilità delle singole banche per l'approvazione dei piani di continuità.
Par. 1 (Destinatari della disciplina)	E' stato suggerito, con riferimento alle banche, di mantenere il testo nell'ambito delle Istruzioni di Vigilanza e, con riferimento agli altri soggetti, di enucleare un testo identico che contenga anche i riferimenti alla continuità operativa inseriti nel Capitolo 7, con riferimento all'*internal audit* e all'esternalizzazione di funzioni aziendali.	In parte	Testo modificato. Le norme sono state inserite in un allegato tecnico applicabile alla generalità degli operatori del settore finanziario. Per quanto attiene alle banche, il Capitolo 9, nel rimandare a tale allegato, ne dettaglia e precisa le modalità applicative. L'estensione delle regole in materia di *business continuity* a soggetti diversi dalle banche avverrà attraverso l'emanazione di disposizioni specifiche che rinvieranno al citato allegato.
	È stato chiesto se: - la normativa sulla continuità operativa si applica anche ai fornitori dei sistemi informativi; - la normativa possa prevedere che gli *outsourcer* siano in possesso di determinate certificazione internazionale che ne attestino il rispetto delle *best practices* di mercato.	Chiarimento	Si fa presente che la disciplina sulla continuità operativa si applica ai soggetti espressamente individuati, tra i quali non rientrano gli *outsourcer* di sistemi informativi; né viene previsto che detti soggetti debbano essere in possesso di determinate certificazioni. Tuttavia, la stessa disciplina - come anche le disposizioni in materia di controlli interni (Capitolo 7) e sistemi

CAPITOLO 9 La continuità operativa			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
			informativi (Capitolo 8) delle banche - detta precise regole in materia di esternalizzazione per assicurare sia che gli incarichi di *outsourcing* siano affidati a soggetti qualificati sia che vengano rispettate le disposizioni in materia di continuità operativa.
Par. 2 (Premessa)	È stato proposto i inserire le seguenti definizioni: - *Tempo obiettivo di ripristino (RTO – Recovery Time Objective):* obiettivo di ripristino in termini di periodo di tempo successivo al verificarsi di un incidente necessario per la ripartenza di un processo a un livello di servizio prestabilito; - *Punto obiettivo di ripristino (RPO – Recovery Point Objective):* obiettivo di ripristino in termini di perdita di dati ammissibile, ovvero periodo di tempo massimo che intercorre tra l'ultimo salvataggio dei dati e il momento di blocco del processo che li utilizza. - *Tempo massimo accettabile di interruzione del servizio:* tempo oltre il quale diventa inaccettabile l'impatto negativo derivante da una interruzione di servizio conseguente a una situazione sfavorevole.	In parte	Il testo è stato rivisto. In merito alle osservazioni ricevute, si fa presente che: - il tempo di ripristino è calcolato a partire dalla di dichiarazione formale dello stato di crisi; - il tempo massimo accettabile di interruzione non è inserito tra le definizioni perché non è citato nel testo normativo.
	È stato suggerito di fare riferimento agli standard elaborati da parte di organismi internazionali in materia (ISO 22301).	In parte	Il testo è stato modificato, senza tuttavia citare esplicitamente i singoli standard.
	È stato chiesto di precisare che nell'ambito oggettivo della "continuità operativa" rientra anche la qualità di scrittura del *software*, quale componente strategica per la stabilità dei servizi di *application management*. Inoltre, è stato suggerito di precisare il concetto di "prolungati disservizi".	No	Con riguardo al primo punto, si osserva che nel concetto di continuità operativa non rientra anche la scrittura del *software*, in quanto le disposizioni fanno riferimento ai servizi, non alle tecnologie. Il punto è stato, peraltro, trattato nel Capitolo 8 (Il sistema informativo). Per quanto riguarda, invece, la definizione di "prolungato disservizio", si ritiene che tale definizione debba essere sufficientemente elastica per essere applicabile ai

CAPITOLO 9 La continuità operativa			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
			vari servizi prestati.
Par. 4 (Ambito del piano di continuità operativa)	È stato rilevato che la locuzione "*alterazione dei dati o indisponibilità dei sistemi a seguito di attacchi perpetrati dall'esterno attraverso reti telematiche*", rischia di limitare l'indisponibilità dei sistemi ICT al solo evento di attacchi provenienti dall'esterno. È stato pertanto suggerito di separare tale punto in due componenti, l'una focalizzata sulla fattispecie in cui si verifica l'alterazione di dati (integrando tale previsione con la specificazione della semplice indisponibilità dei dati e inserendo inoltre il riferimento ai "documenti critici"), l'altra, riferita ai sistemi informativi, che estende l'indisponibilità alle varie possibili cause. In particolare, è stato proposto di modificare il quarto alinea del punto elenco come segue: - alterazione o perdita di dati e documenti critici; - indisponibilità dei sistemi informativi critici.	Sì	Testo modificato.
	Tra gli scenari di crisi è prevista l'eventualità che si verifichino "*danneggiamenti gravi provocati da dipendenti*". In ordine a tale scenario, sono state proposte due riflessioni: l'approccio alla continuità operativa è tipicamente per impatti legati all'indisponibilità di una risorsa critica e lo scenario qui proposto può essere agevolmente ricondotto all'indisponibilità delle risorse danneggiate; da un punto di vista gestionale, la specificità attribuibile ai danneggiamenti provocati dai dipendenti è attentamente analizzata nell'ambito del rischio operativo e della sicurezza informatica. Pertanto, è stato proposto di eliminare tale eventualità tra gli scenari di crisi previsti dalle disposizioni.	Sì	Testo modificato.

CAPITOLO 9 La continuità operativa			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	È stato richiesto di accennare al fatto che gli scenari di crisi, una volta manifestatisi, possono produrre perdite economiche che daranno l'avvio al processo di analisi *ex post* delle cause per l'associazione agli *Event Type* che, nel caso specifico, li avranno generati.	Chiarimento	Si condivide l'esigenza di creare sinergie tra le attività relative alla continuità operativa e quella connessa alla gestione dei rischi operativi. Tuttavia, si ritiene che tali aspetti non riguardino la disciplina della continuità operativa, ma vadano più opportunamente trattati nella disciplina del sistema dei controlli interni e dei rischi operativi, che già prevedono opportuni flussi informativi dalle diverse funzioni aziendali.
	È stato suggerito di inserire un riferimento alla fase di rientro alla normalità dopo un evento disastroso.	Sì	Testo modificato.
Par. 5 (Correlazione ai rischi)	È stato chiesto di chiarire che i rischi residui devono essere accettati dall'organo con funzione di supervisione strategica (nella formulazione attuale è previsto che devono *"essere accettati dall'intermediario"*).	Sì	Testo modificato.
	È stato suggerito di chiarire che i "*i rischi residui non gestiti dal piano rientrano nelle valutazioni delle componenti di alcune metriche del risk appetite/risk tolerance (componente di assorbimento di capitale da "rischio operativo PILLAR 1 – Advanced Measurement Approach - AMA)…"*.	No	Si ritiene che tale previsione non sia coerente con l'oggetto della disciplina in materia di continuità operativa. Rimane ferma, invece, l'applicazione delle disposizioni in materia di rischi operativi e, più in generale, di sistema di controllo dei rischi, nel cui ambito dovranno essere gestiti i rischi residui non gestiti dal piano.
Par. 6 (Definizione del piano e gestione dell'emergenza)	E' stato suggerito di ripristinare il paragrafo relativo alle responsabilità degli organi aziendali.	Sì	Testo modificato.

CAPITOLO 9 La continuità operativa			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
Par. 6.1 (I processi critici)	Nell'ambito dell'attribuzione delle responsabilità legate alle misure di continuità dei processi critici, si ritiene opportuno dare maggiore enfasi alla necessità che il responsabile del processo operi in pieno accordo con le misure stabilite nel piano di continuità. A tal fine si propone la seguente modifica: "*Il responsabile del processo, **in accordo con gli indirizzi strategici e con le regole stabilite nel piano**, individua il tempo massimo accettabile di interruzione del servizio e collabora attivamente alla realizzazione delle misure di continuità ~~in accordo con gli indirizzi strategici e con le regole stabilite nel piano~~.".*	Sì	Testo modificato.
Par. 6.2 (La responsabilità del piano)	Allo scopo di assicurare l'omogeneità dei termini utilizzati con riferimento alla continuità operativa, è stato proposto di adottare sempre le diciture "stato di crisi" anziché "stato di emergenza" e "piano di continuità operativa" anziché "piano di emergenza".	Sì	Testo modificato.
Par. 6.3 (Il contenuto del piano)	E' stato proposto di modificare il quinto capoverso come segue: *"La frequenza dei back-up è correlata al volume di operatività dell'intermediario; gli archivi di produzione **dei sistemi critici** sono duplicati almeno giornalmente…".*	In parte	Testo modificato. Il testo è stato integrato per distinguere le modalità di effettuazione dei *back-up* dei sistemi di supporto ai processi critici rispetto agli altri sistemi.
Par. 6.4 (Le verifiche)	È stato rilevato che l'estensione raggiunta dai piani di continuità operativa in termini di processi critici rende sempre più articolati i piani dei test messi in atto dalle banche. Nell'esperienza comune a un test tecnico (*Disaster Recovery*) svolto nelle modalità definite dalla normativa, si affiancano esercitazioni più complessive che, simulando uno o più scenari, testano anche misure organizzative. Per tale ragione, è stato suggerito di estendere la terminologia adottata per riflettere tale approccio, contemperando allo stesso tempo la possibilità di una rotazione dei processi sottoposti a verifica ogni anno. È stato proposto di modificare il paragrafo come segue: *"Le verifiche delle misure di **continuità operativa** ~~emergenza~~ sono correlate ai rischi e alle criticità dei processi; di conseguenza sono*	No	Si ritiene opportuno mantenere il requisito di almeno una verifica annuale complessiva perché le singole prove settoriali non necessariamente colgono la complessità dei processi di attivazione a livello aziendale. Inoltre, è importante verificare le prestazioni e non solo l'attivazione dei siti secondari per verificare che essi siano in grado di gestire i normali volumi operativi.

CAPITOLO 9 La continuità operativa			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	ipotizzabili differenti frequenze e livelli di dettaglio delle prove. In alcuni casi può essere sufficiente la simulazione parziale dell'evento catastrofico; per i processi più critici le verifiche prevedono il coinvolgimento degli utenti finali, degli outsourcer e, qualora possibile, delle controparti rilevanti. Con frequenza almeno annuale ***vengono svolte*** *~~viene~~ ~~svolta~~ ~~una~~* ***verifiche*** *~~complessiva~~, il più possibile* ***realistiche****, del ripristino della operatività* ***dei processi critici*** *~~condizioni~~ ~~di emergenza~~, effettuando il controllo della funzionalità ~~e delle prestazioni dei sistemi secondari~~ e riscontrando la capacità dell'organizzazione di attuare nei tempi previsti le misure definite nel piano".*		
	È stato fatto presente che l'esecuzione delle procedure *batch* durante le verifiche effettuate con dati a perdere non può essere completa in quanto non può comprendere lo scambio di flussi con l'esterno; in tal senso, è stato proposto di modificare il terzo capoverso come segue: *"In particolare, le verifiche annuali dei sistemi informativi devono prevedere l'attivazione dei collegamenti di rete presso il sito secondario,* ***l'attivazione*** *~~l'esecuzione~~* ***di*** *~~delle~~ procedure batch e – per le banche - l'operatività on-line di almeno una succursale".*	In parte	La disposizione richiede che le verifiche siano effettuate con dati di produzione. Per rendere esplicita tale circostanza il testo è stato integrato.
Par. 6.5 (Le risorse umane)	È stato chiesto di integrare il testo del documento di consultazione come segue: *"Le procedure di emergenza sono chiare e dettagliate, in modo da poter essere eseguite anche da risorse non* ***impegnate nell'ordinario in tali attività*** *~~esperte~~".*	Sì	Testo modificato.
Par. 6.8 (Comunicazioni alla Banca d'Italia)	Il paragrafo prevede che in caso di incidente grave l'intermediario debba informare tempestivamente la Banca d'Italia; tuttavia, è stato fatto presente che il testo non integra le successive disposizioni trasmesse dalle filiali della Banca d'Italia alle banche operanti nei rispettivi territori. E' stato suggerito di modificare le disposizioni per	Sì	Testo modificato.

CAPITOLO 9 La continuità operativa			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
	chiarire tale aspetto.		
Par. 7.1 (Processi a rilevanza sistemica)	È stato chiesto di precisare che i sevizi che si caratterizzano come processi a rilevanza sistemica sono indicati agli intermediari in modo nominativo.	Sì	Testo modificato.
	È stato chiesto di chiarire che, nell'ambito dei processi a rilevanza sistemica, i servizi volti a soddisfare le esigenze di liquidità degli operatori economici non sono compromessi dalla indisponibilità dei punti di erogazione di un singolo intermediario, ma dalla indisponibilità dell'intero circuito.	Sì	Testo modificato.
	È stato chiesto di chiarire il motivo per il quale è stata eliminata la distinzione fra servizi vitali, critici e non critici.	Chiarimento	La classificazione dei processi d'interesse per la continuità operativa è stata articolata su due livelli (critici e sistemici) in modo da uniformare le disposizioni attualmente vigenti per le banche e per gli altri operatori.
Par. 7.5 (Tempi di ripristino e percentuali di disponibilità)	È stato chiesto di chiarire che il processo di dichiarazione dello stato di crisi deve essere formalizzato e consentire di assumere decisioni in tempi coerenti con i tempi di ripristino.	In parte	Testo modificato. Le disposizioni sono state riviste per chiarire che: - il processo di gestione della continuità operativa è integrato con quello di gestione degli incidenti (cfr. Capitolo 8); entrambi prevedono efficaci procedure di *escalation*; - il processo per la dichiarazione dello stato di crisi include una tempestiva comunicazione alla Banca d'Italia; - il processo di ripristino include le attività di: i) analisi degli interventi tecnici e organizzativi da attuare per fronteggiare la crisi; ii) ripartenza attraverso l'attuazione degli opportuni interventi tecnici e/o or-

CAPITOLO 9 La continuità operativa			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/in parte/Chiarimento)	COMMENTO
			ganizzativi e successiva verifica della correttezza delle attività svolte. Inoltre, è previsto che, per i processi a rilevanza sistemica, il tempo di ripristino sia contenuto entro quattro ore, mentre il tempo di ripartenza non superi le due ore.
	È stato chiesto di chiarire il ruolo del coordinamento interbancario posto in essere dalla Banca d'Italia nell'ambito del CODISE, in particolare nei casi in cui si verifichino situazioni di particolare gravità che possono mettere a rischio il rispetto dei tempi di ripristino.	Sì	Testo modificato.
Par 8 (Comunicazioni alla Banca d'Italia)	È stato chiesto di chiarire che il paragrafo si riferisce esclusivamente ai processi a rilevanza sistemica.	Sì	Testo modificato.

Periodo transitorio

Periodo transitorio			
ARGOMENTO	OSSERVAZIONE	VALUTAZIONE (Sì/No/In parte/Chiarimento)	COMMENTO
Tempistica e periodo transitorio	È stato chiesto un congruo periodo di tempo per l'entrata in vigore delle disposizioni. In particolare, sono stati suggeriti: – un termine di 6 mesi per la pianificazione degli interventi che ciascun intermediario deve effettuare; – un termine variabile (anche di 12 mesi per i casi più critici), da concordare con ciascun intermediario, per l'implementazione delle misure individuate in fase di pianificazione. È stato chiesto di prevedere, in ossequio al principio di gradualità, un'adeguata flessibilità dei tempi di implementazione dei processi di valutazione delle attività aziendali per permettere la definizione e attuazione delle iniziative, a livello di Sistema, necessarie per supportare l'adeguamento delle banche di Categoria.	Sì	L'atto di emanazione delle disposizioni prevede una dettagliata disciplina transitoria.