BANCA D'ITALIA
EUROSISTEMA

IL SISTEMA DEI CONTROLLI INTERNI, IL SISTEMA INFORMATIVO E LA CONTINUITÀ OPERATIVA

Nota di chiarimenti ([1]) ([2])

Nella presente nota vengono forniti alcuni chiarimenti in merito all'applicazione della disciplina in materia di sistema dei controlli interni, sistema informativo e continuità operativa delle banche e dei gruppi bancari, contenuta nella Circolare n. 285 del 19 dicembre 2013, Parte Prima, Titolo IV, Capitoli 3, 4 e 5.

DISPOSIZIONI TRANSITORIE (Comunicazione del 2 luglio 2013 – Bollettino di vigilanza n. 7, luglio 2013)

1. *Il documento di autovalutazione (*gap analysis*) è redatto a livello consolidato o è necessario redigere anche documenti individuali per ciascuna componente del gruppo?*

   Ciascuna componente bancaria italiana del gruppo redige il documento di *gap analysis* sulla base delle disposizioni applicabili. La trasmissione alla Banca d'Italia è curata dalla capogruppo che, oltre a fornire una visione consolidata della situazione del gruppo rispetto alle previsioni normative (Capitolo 3, Sezione V), consolida in un unico documento le *gap analysis* individuali.

2. *Il perimetro del documento consolidato di* gap analysis *ha come riferimento la verifica del rispetto dei nuovi requisiti per le sole banche o anche per le componenti del gruppo non bancarie? È necessario condurre l'analisi anche con riferimento alle controllate estere?*

   Il documento di *gap analysis* è diretto a valutare il grado di aderenza degli assetti organizzativi e di controllo delle banche e dei gruppi bancari rispetto alle previsioni normative e a indicare le azioni che tali soggetti intendono intraprendere per assicurare il pieno rispetto della normativa. Le componenti non bancarie dei gruppi e le controllate estere, non rientrando tra i destinatari della disciplina in esame, non sono tenute a redigere il documento di *gap analysis*, rimanendo soggette alle disposizioni organizzative specifiche loro eventualmente applicabili.

   Ciò posto, la capogruppo, secondo quanto previsto dal Capitolo 3, Sezione V, nel valutare l'adeguatezza del sistema dei controlli del gruppo, tiene conto di tutte le componenti del gruppo bancario, incluse quelle non bancarie e le controllate estere, ed esercita i propri poteri di direzione e controllo per assicurare l'adeguatezza del sistema dei controlli di tali soggetti. Il documento di autovalutazione del gruppo, in una prospettiva consolidata, dà conto della situazione dell'intero gruppo, incluse le componenti che non rientrano tra i destinatari diretti della disciplina.

---

[1] Nota di chiarimenti del 24 gennaio 2014, aggiornata al 6 giugno 2014 e successivamente al 22 luglio 2015 e al 6 febbraio 2017.

[2] Le parti di testo tra parentesi quadre sono da ritenersi abrogate.

3. *L'elenco degli accordi di esternalizzazione in essere deve essere inviato dalla capogruppo per tutte le componenti del gruppo o deve essere inviato individualmente?*

L'elenco è inviato dalla capogruppo, con riferimento a tutti gli accordi di esternalizzazione in essere soggetti alle nuove disposizioni.

4. *I contratti di esternalizzazione conclusi dopo l'entrata in vigore della nuova disciplina ma prima della data di efficacia entro quale termine devono essere adeguati? Per tali contratti deve essere inviata la comunicazione alla Banca d'Italia?*

I contratti di esternalizzazione conclusi dopo l'entrata in vigore della nuova disciplina (3 luglio 2013) devono essere adeguati alle nuove disposizioni entro e non oltre la data di efficacia delle disposizioni (1° luglio 2014). Entro tale data le banche inviano alla Banca d'Italia una comunicazione che indica tutti i contratti stipulati nel periodo compreso tra la data di entrata in vigore delle disposizioni e la data della loro efficacia .

5. *Le filiali di banche comunitarie devono effettuare la* gap analysis*?*

Le filiali di banche comunitarie sono tenute a effettuare la *gap analysis* con riferimento alle disposizioni di cui sono destinatarie (cfr. Capitolo 3, Sezioni VII e IX), che prevedono l'obbligo di condurre una verifica annuale circa: (a) l'adeguatezza delle procedure interne rispetto all'obiettivo di prevenire la violazione delle norme italiane applicabili; (b) la conformità della condotta aziendale rispetto alle norme italiane applicabili alla succursale.

6. *Entro quali termini le banche dovranno redigere il piano di audit pluriennale e la relazione di verifica sulle attività esternalizzate?* ([3])

Il piano di *audit* pluriennale dovrà essere redatto e approvato entro la chiusura dell'esercizio in cui la nuova disciplina è divenuta efficace.

Con riferimento alla relazione relativa ai controlli svolti sulle attività esternalizzate, la stessa dovrà essere redatta e comunicata alla Banca d'Italia, per la prima volta, entro il 30/04/2015.

PRINCIPI GENERALI (Parte Prima, Titolo IV, Capitolo 3, Sezione I)

1. *Con riferimento alle politiche e procedure di gestione delle risorse umane, è stato chiesto se dette politiche e procedure devono essere racchiuse in una specifica* policy *o può considerarsi sufficiente prevedere che ogni delibera avente per oggetto la gestione delle risorse umane sia adeguatamente formalizzata e contenga specificamente le motivazioni e le finalità poste alla sua base?* ([4])

Le politiche e le procedure di gestione delle risorse umane sono riportate in una specifica *policy* aziendale approvata dall'organo con funzione di supervisione strategica. La *policy* è volta ad assicurare che il personale sia provvisto delle competenze e delle professionalità necessarie per l'esercizio delle responsabilità a

[3] Aggiornamento del 6 giugno 2014.
[4] Aggiornamento del 6 giugno 2014.

esso attribuite. I successivi atti gestionali devono essere coerenti con la *policy* adottata.

2. *È previsto che i processi e le metodologie di valutazione delle attività aziendali siano "affidabili e integrati con il processo di gestione del rischio". In proposito, è stato chiesto: i) se sia corretto ritenere che la norma si applichi solo qualora le disposizioni IAS/IFRS lascino spazi di manovra o differenti opzioni alla banca nella valutazione delle attività aziendali; ii) quali siano i rischi impattati da eventuali errate metodologie di valutazione delle attività aziendali; iii) quale sia la metrica attraverso cui valutare il rischio di non corretta valutazione contabile.* ([5])

   Con riguardo al primo quesito, si fa presente che la norma si applica anche nei casi in cui i principi contabili non lascino margini di discrezionalità. Rimane, infatti, fermo il principio secondo cui la banca deve assicurare l'affidabilità dei processi e delle metodologie di valutazione e la relativa integrazione con il processo di gestione dei rischi. Si veda anche il Resoconto della consultazione, pag. 14.

   Quanto al secondo profilo, l'errata valutazione delle attività aziendali, anche solo a fini gestionali, può impattare su diverse tipologie di rischio (finanziari, legali, operativi, reputazionali).

   Per quanto, infine, concerne le metriche attraverso cui valutare il rischio di non corretta valutazione delle attività aziendali, la definizione e lo sviluppo delle stesse sono rimessi all'autonomia organizzativa delle banche.

3. *A chi compete la verifica del grado di aderenza ai requisiti del sistema dei controlli interni e dell'organizzazione, stante il generico riferimento della sua attribuzione alle "banche" presente nella norma? Con quali modalità deve essere formalizzata la verifica? Essa rappresenta un'ulteriore verifica rispetto a quella avente ad oggetto la valutazione periodica sulla completezza, adeguatezza, funzionalità e affidabilità del sistema dei controlli interni?* ([6])

   Le banche assicurano la completezza, l'adeguatezza, la funzionalità e l'affidabilità del sistema dei controlli interni (ossia "il grado di aderenza ai requisiti del sistema") e il rispetto dei particolari principi di organizzazione. La responsabilità primaria è rimessa agli organi aziendali, ciascuno secondo le proprie competenze e responsabilità; le modalità di esecuzione delle suddette attività sono quelle proprie delle attività degli organi aziendali.

RUOLO DEGLI ORGANI AZIENDALI (Parte Prima, Titolo IV, Capitolo 3, Sezione II)

1. *Per i gruppi bancari è sufficiente redigere un unico documento di coordinamento dei controlli (Sezione II, par.5), redatto a livello consolidato o è invece necessario che ciascuna componente bancaria del gruppo rediga detto documento?*

   Ciascuna componente bancaria del gruppo – in quanto destinataria della disciplina a livello individuale – è tenuta a redigere il documento di coordinamento dei controlli.

[5] Aggiornamento del 6 giugno 2014.
[6] Aggiornamento del 6 giugno 2014.

La capogruppo, a sua volta, redige il documento di coordinamento dei controlli del gruppo, che tiene conto del complessivo assetto dei controlli del gruppo. In tale ambito, la capogruppo assicura, tra l'altro, la coerenza tra i documenti di coordinamento redatti a livello individuale e il documento redatto a livello di gruppo.

2. *Un organismo di vigilanza ex d.lgs. 231/2001 composto dal presidente del collegio sindacale, dal responsabile della* compliance *e dal responsabile dell'*internal audit *è ritenuto coerente con le nuove disposizioni?* ([7])

La Circ. 285/2013 riconosce alle banche la facoltà di affidare le funzioni dell'organismo di vigilanza ex d.lgs. 231/2001 a un organismo appositamente costituito, previa adeguata motivazione. L'adeguatezza della motivazione va valutata alla luce dell'idoneità della particolare composizione prescelta per l'organismo ad assicurare il corretto espletamento dei compiti a esso attribuiti e un efficace coordinamento con il sistema dei controlli interni. Fermo restando l'autonomia della banca e le valutazioni della Vigilanza sui casi concreti, la presenza dei responsabili delle funzioni aziendali di controllo di secondo e terzo livello e del presidente dell'organo con funzione di controllo non appare incoerente con i principi della regolamentazione volti a favorire, come detto, il coordinamento tra i vari soggetti preposti ai compiti di controllo e ad assicurare un adeguato grado di autonomia e indipendenza dell'organismo.

3. *Il processo di gestione del rischio è un elemento autonomo e separato rispetto al RAF e alla* policy *di governo dei rischi?* ([8])

La politica di governo dei rischi rappresenta una componente strategica del RAF, consentendone il raccordo con il complessivo piano strategico. Il processo di gestione dei rischi, invece, concorre all'attuazione del RAF.

4. *Con riferimento al sistema dei controlli interni, nelle banche di credito cooperativo, è possibile delegare alcuni compiti dell'organo con funzione di gestione al direttore generale?* ([9])

L'organo con funzione di gestione è l'organo aziendale o i componenti di esso a cui – ai sensi del codice civile o per disposizione statutaria – spettano o sono delegati compiti di gestione, intesa come attuazione degli indirizzi deliberati nell'esercizio della funzione di supervisione strategica. Con riferimento al sistema dei controlli interni, l'organo con funzione di gestione è assegnatario di precisi compiti e responsabilità previsti nella Sezione II, par. 3, non delegabili ad altri soggetti fra cui anche il direttore generale, che rappresenta il vertice della struttura interna dell'intermediario.

[7] Aggiornamento del 6 giugno 2014.
[8] Aggiornamento del 6 giugno 2014.
[9] Aggiornamento del 6 giugno 2014.

FUNZIONI AZIENDALI DI CONTROLLO (Parte Prima, Titolo IV, Capitolo 3, Sezione III)

1. *Nelle banche di piccole dimensioni o a limitata complessità operativa, sprovviste di un amministratore delegato e di un comitato esecutivo, le funzioni aziendali di controllo di secondo livello possono essere collocate a riporto gerarchico del direttore generale?*

   Le funzioni aziendali di controllo di secondo livello devono essere collocate alle dirette dipendenze dell'organo con funzione di gestione. Il direttore generale, pur partecipando alla funzione di gestione, non può essere identificato con l'organo stesso che, invece, nei casi prospettati è da individuarsi nel consiglio di amministrazione. Il direttore generale, proprio perché rappresenta il vertice della struttura interna e partecipa alla funzione di gestione, è destinatario dei flussi informativi previsti per gli organi aziendali nonché, nelle banche di dimensioni molto contenute e prive di un amministratore delegato o di un comitato esecutivo, può svolgere un ruolo di raccordo funzionale tra le funzioni aziendali di controllo di secondo livello e l'organo con funzione di gestione, da cui dipendono gerarchicamente le citate funzioni.

2. *[Quali sono le disposizioni del Capitolo 3 applicabili alle "funzioni aziendali di controllo" individuate nella Sezione I, paragrafo 3, lettera g), nota 1 (cioè "funzione antiriciclaggio" e "funzione di convalida"), alla luce dell'ultima frase riportata nella citata nota ("Tali funzioni sono disciplinate dalle citate disposizioni e, in quanto compatibili, dal presente Capitolo")? In particolare, sono applicabili le disposizioni riguardanti la collocazione gerarchica dei responsabili?*

   La nota 1 del paragrafo 3 prevede che tra le "funzioni aziendali di controllo" rientrino - oltre alle funzioni di conformità alle norme, di controllo dei rischi e di revisione interna - anche la funzione antiriciclaggio e la funzione di convalida e che tali ultime funzioni siano disciplinate dalle loro specifiche previsioni di settore e, in quanto compatibili, dalle disposizioni del Capitolo 3. A tal fine, il giudizio di compatibilità concerne solo quelle disposizioni che attengono a materie non regolate dai provvedimenti specifici che disciplinano le funzioni in parola. Con particolare riferimento alle disposizioni concernenti la collocazione gerarchica dei responsabili, essendo la materia già regolata nei provvedimenti specifici in materia di "funzione antiriciclaggio" e di "funzione di convalida", queste trovano applicazione solo con riferimento alle funzioni di *compliance*, *risk management* e *internal audit*.] ([10]) ([11]).

3. *Sulle operazioni di maggior rilievo di diretta competenza dell'OFSS o dell'OFG, il parere del* risk management *deve essere acquisito almeno a fini consultivi?* ([12])

   La Circ. 285/2013 prevede espressamente che la funzione di *risk management* sia chiamata, fra l'altro, a fornire pareri preventivi sulla coerenza delle operazioni di maggiore rilievo - individuate secondo i criteri definiti e approvati dall'organo con funzione di supervisione strategica - con il RAF.

---

[10] Aggiornamento del 22 luglio 2015.

[11] L'11° aggiornamento della Circ. 285 ha modificato la nota 1 contenuta nella Circ. 263 (rinumerata nella nuova Circolare come nota 3) in base alla quale era previsto che la funzione di antiriciclaggio e quella di convalida, oltre a essere disciplinate dalle loro specifiche previsioni di settore, erano regolate dalle disposizioni del Capitolo 3 in quanto compatibili.

[12] Aggiornamento del 6 giugno 2014.

Fermo restando che la disciplina non richiede in via obbligatoria l'acquisizione del parere del *risk management* riguardo alle operazioni che rientrano nella diretta competenza degli organi di supervisione strategica e di gestione, la richiesta in tali circostanze di pareri consultivi al *risk management* può rappresentare una buona prassi gestionale.

4. *È ammissibile che i responsabili delle funzioni aziendali di controllo di secondo livello riportino gerarchicamente a un componente dell'organo amministrativo?* ([13])

Il par. 1, lett b), secondo alinea, stabilisce che i responsabili delle funzioni di controllo dei rischi e di conformità alle norme (funzioni aziendali controllo di secondo livello) sono collocati alle dirette dipendenze dell'organo con funzione di gestione o dell'organo con funzione di supervisione strategica.

Con riferimento all'organo con funzione di gestione, esso si identifica con l'organo aziendale nella sua interezza o con i componenti di esso ai quali spettano o sono delegati compiti di gestione; pertanto, il riporto gerarchico dei responsabili verso un solo componente dell'organo amministrativo è ammesso solo se tale amministratore sia identificabile con l'organo con funzione di gestione.

5. *Quali sono l'ambito e le modalità di presidio della funzione di conformità rispetto alla c.d.* compliance *IT?* ([14])

La funzione di conformità è assegnataria delle responsabilità in merito allo svolgimento dei controlli di secondo livello concernenti il rispetto dei regolamenti interni e delle normative esterne in tema di ICT (ICT *compliance*). Resta ferma la possibilità per la funzione di *compliance* di avvalersi delle forme di flessibilità previste dal par. 3.2, quali l'utilizzo di risorse specializzate appartenenti ad altre strutture.

6. *L'incarico di responsabile della funzione di conformità può essere conferito tramite un contratto di lavoro a progetto?* ([15])

Il responsabile della funzione di *compliance*, per il ruolo e le responsabilità che gli sono attribuiti, deve essere un elemento stabile dell'organigramma aziendale, in possesso di un'adeguata autorevolezza che gli consenta di esercitare le sue prerogative in maniera efficace e indipendente. La forma contrattuale da adottare per conferire l'incarico di responsabile, rimessa all'autonomia negoziale delle parti, deve essere coerente con tali principi e non deve essere volta a eludere la specifica disciplina dell'esternalizzazione di attività aziendali.

7. *Il direttore generale di una società controllata può assumere l'incarico di responsabile della funzione di* compliance *di gruppo, nel caso in cui la società controllata venga esclusa dal perimetro della funzione di* compliance *di gruppo?* ([16])

Il par. 1, lett. b) prevede espressamente che il responsabile della funzione di *compliance* non possa avere responsabilità dirette in aree operative sottoposte a controllo. Né può ritenersi ammissibile una limitazione artificiosa del perimetro di

[13] Aggiornamento del 6 giugno 2014.
[14] Aggiornamento del 6 giugno 2014.
[15] Aggiornamento del 6 giugno 2014.
[16] Aggiornamento del 6 giugno 2014.

competenza della *compliance*, che non coincida con l'estensione effettiva dell'ambito di operatività del gruppo bancario. Si ritiene, dunque, che nel caso di specie l'incarico di responsabile della *compliance* non possa essere affidato al direttore generale della società controllata.

8. *Quali sono le modalità con le quali possono essere sviluppati ed applicati gli indicatori in grado di evidenziare situazioni di anomalia o di inefficienza dei sistemi di misurazione e controllo dei rischi?* ([17])

La Circ. 285/2013 dispone che le banche assicurino la completezza, l'adeguatezza, la funzionalità e l'affidabilità del sistema dei controlli interni, utilizzando presidi in grado di coprire ogni tipologia di rischio aziendale e secondo definiti compiti e responsabilità.

Le banche sono tenute ad applicare le disposizioni in materia secondo il principio di proporzionalità, tenuto conto, dunque, delle proprie peculiari caratteristiche operative.

Pertanto, rientra nell'autonomia di ciascuna banca definire, sulla base della propria operatività aziendale e del relativo profilo di rischio, gli indicatori in grado di evidenziare situazioni di anomalia o di inefficienza dei sistemi di misurazione e controllo dei rischi.

9. *Qualora il sistema informativo sia affidato in full outsourcing, è corretto ritenere che la funzione di revisione interna possa affidarsi alle verifiche effettuate dall'auditor della società fornitrice del servizio. In ogni caso, è possibile avere qualche orientamento sull'eventuale ruolo e compiti del referente per le attività esternalizzate nell'ambito dell'ICT* audit*?* ([18])

La Circ. 285/2013 prevede espressamente che, tenuto conto del principio di proporzionalità, per le verifiche sui componenti o servizi ICT esternalizzati, la funzione di audit dell'intermediario possa scegliere, sotto la propria responsabilità, di fare affidamento sull'*internal audit* del fornitore di servizi, previa valutazione della sua professionalità e indipendenza (cfr. Capitolo 4, Sezione II, par. 7, nota 7).

In ogni caso, il referente per i sistemi informativi esternalizzati, essendo responsabile del controllo su tale funzione e assumendo il ruolo di "utente responsabile" nel processo di analisi del rischio informatico, deve essere informato delle risultanze degli incarichi di ICT audit e segue l'implementazione delle eventuali misure correttive suggerite; in tale contesto, se necessario, detto referente cura d'intesa con il fornitore l'adeguamento dei parametri e delle procedure di monitoraggio dei livelli di servizio.

10. *Le banche possono ricorrere al modello di* compliance *graduato in materia di* information and communication technology *(ICT)?* ([19])

L'attuale quadro normativo prevede, come regola generale, che la funzione di *compliance* presieda la gestione del rischio di non conformità con riferimento a tutte le norme applicabili alle banche. Le banche, inoltre, nei limiti delle disposizioni normative vigenti, hanno la possibilità di adottare un modello di *compliance* "graduato" attribuendo alcune fasi del processo di *compliance* a uno o più presidi

[17] Aggiornamento del 6 giugno 2014.
[18] Aggiornamento del 6 giugno 2014.
[19] Aggiornamento de 22 luglio 2015.

specializzati. A tal proposito, le disposizioni di vigilanza prevedono che la possibilità di graduare compiti della funzione di *compliance* rappresenta un'eccezione rispetto al principio generale, cui le banche possono ricorrere solo nei casi tassativamente previsti dalla disciplina e, in particolare: i) quando la costituzione di specifici presidi di controllo di conformità sia già prevista espressamente da disposizioni normative ad hoc (come, ad esempio, nei casi della normativa in materia di sicurezza sul lavoro o del trattamento dei dati personali); ii) per far fronte al rischio di non conformità alle normative in materia fiscale. In tali casi, la funzione di *compliance* è responsabile "almeno della definizione delle metodologie di valutazione del rischio di non conformità e della individuazione delle relative procedure, e procede alla verifica dell'adeguatezza delle procedure medesime a prevenire il rischio di non conformità".

Con riguardo alla *compliance* ICT, si fa presente che la normativa (Capitolo 4, Sezione II, par. 6) prevede che la responsabilità delle attività di conformità alle norme nel settore ICT sia ricondotta nell'ambito del sistema dei controlli interni, senza prevedere l'istituzione di presidi specialistici. Ne deriva che la *compliance* ICT – al pari di ogni altra attività di *compliance* al di fuori delle ipotesi sub i) e sub ii) – non ammette il modello di *compliance* "graduato" e, dunque, rientra nei compiti della funzione di conformità alle norme delle banche la verifica del rispetto dei regolamenti interni e delle normative esterne in tema di ICT. Resta fermo, inoltre, quanto indicato nel chiarimento n. 5 del presente sezione, in materia di organizzazione della funzione di *compliance*.

11. *Nel caso in cui la funzione di gestione sia conferita a più soggetti (comitato esecutivo e amministratori delegati), è ammissibile che i responsabili delle funzioni aziendali di controllo di secondo livello riportino gerarchicamente a uno solo di tali soggetti?* ([20])

L'organo con funzione di gestione (OFG) è "*l'organo aziendale o i componenti di esso ai quali spettano o sono delegati compiti di gestione, ossia l'attuazione degli indirizzi deliberati nell'esercizio della funzione di supervisione strategica; il direttore generale rappresenta il vertice della struttura interna e come tale partecipa alla funzione di gestione*" (Capitolo 1, par. 3).

In via generale, la disciplina sul sistema dei controlli interni sottolinea la necessità che l'organo con funzione di gestione abbia una visione unitaria dei rischi aziendali disponendo che lo stesso (ad es., comitato esecutivo, amministratori delegati), per il corretto esercizio dei compiti e delle responsabilità attribuitegli, abbia "*la comprensione di tutti i rischi aziendali (…), e, nell'ambito della gestione integrata, delle loro interrelazioni reciproche e con l'evoluzione del contesto esterno*" (Sezione II, par. 3). Dunque, nell'attribuzione in concreto di specifiche deleghe in materia di gestione dei rischi deve essere in ogni caso garantita un'efficace allocazione dei poteri allo scopo di assicurare una gestione unitaria di tutti i rischi aziendali.

A tal proposito, si rammenta che le banche sono in ogni caso tenute ad applicare le disposizioni sul governo societario (Capitolo 1, Sezione III) che, tra l'altro, prevedono che "*la contemporanea presenza di un comitato esecutivo e di un amministratore delegato o quella di più amministratori delegati, si giustifica nelle banche di maggiori dimensioni o complessità operativa e richiede una ripartizione chiara delle competenze e delle responsabilità*". Anche per le banche di minore complessità, le

[20] Aggiornamento del 22 luglio 2015.

stesse disposizioni chiariscono che occorre evitare di "*rendere pletorico l'assetto dell'esecutivo*".

Alla luce di quanto sopra, per assicurare una visione e una gestione unitaria dei rischi aziendali, le disposizioni prevedono che le funzioni aziendali di controllo di secondo livello dipendano direttamente dall'organo con funzion e di supervisione strategica o dall'organo con funzione di gestione ([21]) (Sezione III, par. 1, lett. b). In quest'ultimo caso, ai fini della disciplina sui controlli interni, l'organo aziendale titolare della funzione di gestione si identifica con tutti i soggetti ai quali sono attribuiti i compiti declinati nella Sezione II, par. 3. Ne deriva che se, come nel caso prospettato, compiti in materia di gestione dei rischi aziendali, così come individuati nel citato par. 3, sono attribuiti sia al comitato esecutivo sia all'amministratore delegato, le funzioni aziendali di controllo di secondo livello sono poste alle dirette dipendenze di entrambi.

ESTERNALIZZAZIONE (Parte Prima, Titolo IV, Capitolo 3, Sezione IV e Sezione V, par. 3)

1. *Una banca che presta servizi ad altre banche è da considerarsi un fornitore di servizi e quindi soggetta alla disciplina sull'esternalizzazione, anche nel caso in cui i due soggetti appartengano alla medesima associazione di categoria?*

   La disciplina sull'esternalizzazione si applica a prescindere dalla natura del fornitore di servizi. Le uniche eccezioni previste sono quelle concernenti l'esternalizzazione nell'ambito del gruppo bancario e l'esternalizzazione presso associazioni di categoria, fattispecie per le quali, al ricorrere di determinate condizioni, è possibile applicare una disciplina *ad hoc*.

2. *Nei gruppi bancari, oltre alla politica sull'esternalizzazione redatta dalla capogruppo, è necessario che le componenti bancarie del gruppo redigano proprie politiche individuali sull'esternalizzazione?* ([22])

   In presenza di gruppi bancari, le singole componenti bancarie sono tenute alla definizione della politica aziendale in materia di esternalizzazione verso fornitori di servizi non appartenenti al gruppo bancario, tenuto conto delle indicazioni fornite dalla capogruppo nell'ambito del potere di direzione e coordinamento (cfr. Sezione V, par. 2). Per le esternalizzazioni all'interno del gruppo bancario, invece, le singole componenti bancarie, ferme restando le responsabilità per le attività esternalizzate, possono non redigere la politica aziendale in materia di esternalizzazione, se adottano e rispettano la politica aziendale in materia di esternalizzazione redatta dalla capogruppo per il gruppo bancario (cfr. Sezione V, par. 3).

3. *La politica di esternalizzazione di gruppo deve essere redatta con riferimento alle sole componenti bancarie del gruppo o con riferimento a tutte le entità appartenenti al gruppo bancario (Sezione V)?* ([23])

[21] Resta ferma la possibilità per i responsabili delle funzione aziendali di controllo di secondo livello di accedere direttamente all'organo con funzione di supervisione strategica e all'organo con funzione di controllo e di comunicare con questi ultimi senza restrizioni o intermediazioni (Sezione III, par. 1)

[22] Aggiornamento del 6 giugno 2014.

[23] Aggiornamento del 6 giugno 2014.

La politica di esternalizzazione redatta dalla capogruppo deve riguardare tutte le componenti del gruppo.

4. Quali sono esempi di funzioni operative importanti? ([24])

Secondo quanto previsto dalla Sezione I, par. 3, lett. i), sono funzioni operative importanti quelle funzioni per le quali risulta verificata almeno una delle seguenti condizioni:

- un'anomalia nella sua esecuzione o la sua mancata esecuzione possono compromettere gravemente almeno uno tra i seguenti: a) i risultati finanziari, la solidità o la continuità delle attività della banca; b) la capacità della banca di conformarsi alle condizioni e agli obblighi derivanti dalla sua autorizzazione o agli obblighi previsti dalla disciplina di vigilanza;
- attività sottoposte a riserva di legge;
- riguarda processi operativi delle funzioni aziendali di controllo o ha un impatto significativo sulla gestione dei rischi aziendali.

Rientra nella responsabilità delle banche l'individuazione delle funzioni aziendali per le quali sussistono le condizioni previste dalla normativa e che quindi si qualificano come funzioni operative importanti. A titolo meramente esemplificativo, rientrano tra le funzioni operative importanti le funzioni di *back office*, il servizio archivio digitale e/o cartaceo, il recupero crediti, il sistema informativo, la delega di gestione di proprie attività, il trasporto valori, le segnalazioni di vigilanza.

5. È necessario procedere alla comunicazione preventiva alla Banca d'Italia nei casi in cui si modifichi un contratto di esternalizzazione in essere al solo fine di cambiare il fornitore di servizi? ([25])

La sostituzione del fornitore di servizi è da considerarsi una modifica di un elemento essenziale del contratto; è pertanto necessaria, con riferimento all'esternalizzazione delle funzioni operative importanti, la comunicazione preventiva alla Banca d'Italia. Per l'esternalizzazione di funzioni operative non importanti, resta fermo l'obbligo di rispettare i principi generali e la politica di esternalizzazione adottata dalla banca.

6. In materia di esternalizzazione della funzione di revisione interna, continua a trovare applicazione il provvedimento della Banca d'Italia del gennaio 2001 (cfr. Bollettino di vigilanza n. 1/01)? ([26])

La disciplina dell'esternalizzazione delle funzioni aziendali, introdotta dal 15° aggiornamento della Circ. 263/2006, rappresenta un quadro organico della materia e, pertanto, ai fini della presente normativa, il provvedimento del gennaio 2001 ("Modello dell'organizzazione: esternalizzazione della funzione di internal audit") non è applicabile.

[24] Aggiornamento del 6 giugno 2014.
[25] Aggiornamento del 6 giugno 2014.
[26] Aggiornamento del 6 giugno 2014.

7. *In caso di esternalizzazione della funzione di* internal audit*, il ruolo di referente per l'attività esternalizzata può essere affidato a un componente del consiglio di amministrazione (che partecipa con diritto di voto alle adunanze consiliari riguardanti attività operative sottoposte a controllo)?* ([27])

   Al referente per le funzioni aziendali di controllo esternalizzate si applicano le disposizioni previste nella Sezione III, par. 1, lett. b), fra cui la possibilità che possa essere un componente dell'organo amministrativo, purché sia destinatario di specifiche deleghe in materia e non sia destinatario di altre deleghe che ne pregiudichino l'autonomia. Si ritiene che, nel rispetto di quanto precede, la titolarità del diritto di voto nelle adunanze consiliari non sia preclusiva della possibilità di assumere la qualifica di referente per le funzioni aziendali di controllo esternalizzate.

8. *Nelle realtà non complesse (banche medio piccole) risulta frequente il ricorso all'outsourcing di diverse attività (es.: sistema informativo, trattamento del contante, elaborazione delle buste paga); in tali casi, è coerente con il principio di proporzionalità la nomina di un solo referente o è necessario individuare un referente per ogni attività esternalizzata?* ([28])

   Nell'ambito della disciplina del sistema dei controlli interni, il principio di proporzionalità rappresenta un principio generale per l'interpretazione e l'applicazione delle relative disposizioni.

   In virtù di tale principio, per le banche di minori dimensioni e a ridotta complessità operativa, non vi sono elementi ostativi all'esternalizzazione di più funzioni aziendali con individuazione di un solo referente interno, purché siano rispettati i limiti espressamente previsti dalla disciplina (ad esempio, divieto di cumulare controlli di secondo e terzo livello, o attività operative e attività di controllo) e il referente sia effettivamente in grado di svolgere efficacemente il proprio ruolo con riguardo a più attività esternalizzate.

9. *La possibilità di derogare al divieto di cumulare, per uno stesso fornitore di servizi, incarichi relativi a funzioni aziendali di controllo di secondo e terzo livello per una stessa banca o gruppo bancario previsto per le associazioni di categoria che adottino determinati presidi organizzativi può essere estesa anche a quei fornitori di servizi che adottino presidi organizzativi equivalenti a quelli previsti dalla normativa?* ([29])

   [La deroga prevista dalla disciplina riguarda solo le associazioni di categoria (cfr. Sezione IV, par. 2); quindi, non è possibile applicare la medesima deroga ad altri fornitori terzi di servizi.] ([30]) ([31])

10. *In caso di esternalizzazione delle funzioni aziendali di controllo, il fornitore di servizi può essere il revisore contabile persona fisica o una società di consulenza che svolge*

---

[27] Aggiornamento del 6 giugno 2014.
[28] Aggiornamento del 6 giugno 2014.
[29] Aggiornamento del 6 giugno 2014.
[30] Aggiornamento del 22 luglio 2015.
[31] Si veda Capitolo 3, Sezione IV, par. 2, nota 4 introdotta dall'11° aggiornamento del 21 luglio 2015 della Circolare n. 285.

la sua attività mediante l'opera di soggetti iscritti nell'albo dei revisori dei conti? ([32]) ([33])

L'esternalizzazione delle funzioni aziendali di controllo, nei casi previsti nella Sezione IV, par. 2, è ammissibile esclusivamente verso soggetti terzi quali banche, società di revisione o organismi associativi di categoria (cfr. nota 1). Non è ammissibile, pertanto, che il fornitore di servizi, presso cui si intendono esternalizzare le funzioni aziendali di controllo, possa essere il singolo revisore contabile persona fisica o una società diversa da una società di revisione di cui al decreto legislativo del 27 gennaio 2010, n. 39.

Cfr. Resoconto della consultazione, pag. 54

OSSERVAZIONE	VALUTAZIONE (Sì, No, In Parte, Chiarimento)	COMMENTO
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 associati vi) e di definire i requisiti di professionalità, indi pendenza 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 sol o a soggetti che già istituzionalmente s volgono attività bancaria o attività di controllo sulle banche; inoltre, sono consentite forme di esternalizzazione verso organismi associati vi, riconoscendo il ruolo di supporto di tali organismi verso le banche di minore dimensione.

11. *Nel caso di esternalizzazione della funzione di revisione interna presso la capogruppo, può essere nominato referente della controllata per la funzione di revisione esternalizzata il responsabile dell'unità organizzativa della capogruppo incaricata di svolgere le attività di revisione interna in outsourcing?* ([34])

La disciplina in materia di esternalizzazione di funzioni aziendali di controllo all'interno del gruppo bancario prevede, tra l'altro, la nomina di un referente presso la società del gruppo che esternalizza; tale soggetto deve possedere i requisiti previsti in generale per i responsabili delle funzioni aziendali di controllo (Sezione III, par. 1, lett. b), fra cui l'essere collocato alle dirette dipendenze dell'organo con funzione di supervisione strategica della società esternalizzante.

Tale previsione - ferma restando l'esigenza che il referente riporti funzionalmente alla funzione di controllo esternalizzata, come previsto dalla disciplina (Sezione V, par. 3.1, terzo alinea) - è coerente con la circostanza che l'esternalizzazione, anche all'interno del gruppo bancario, non fa venire meno la responsabilità degli organi

[32] Aggiornamento del 6 giugno 2014.
[33] Aggiornamento del 22 luglio 2015.
[34] Aggiornamento del 6 giugno 2014.

aziendali della società controllata per le attività esternalizzate (cfr. Resoconto della Consultazione pag. 33).

Nel caso di specie, pertanto, la soluzione prospettata – cioè la coincidenza del soggetto responsabile presso la capogruppo dei controlli di *audit* presso la controllata e del referente - è ipotizzabile solo nel caso in cui tale soggetto sia posto alle dirette dipendenze dell'organo con funzione di supervisione strategica della società del gruppo che esternalizza.

12. *Sono pervenuti alcuni quesiti volti a chiarire il corretto inquadramento, a fini prudenziali, dell'attività di gestione di monete metalliche svolta dalle società di servizi nell'ambito di rapporti contrattuali con banche. In particolare, è stato chiesto se l'attività - consistente nel ritiro delle monete metalliche non preventivamente autenticate e confezionate e nel successivo trattamento di autenticazione e selezione tra monete idonee e non idonee alla circolazione attraverso apparecchiature conformi alla normativa, con successiva "restituzione" alle banche del "controvalore delle monete metalliche" riscontrate autentiche e idonee - si configuri come "esternalizzazione" da parte delle banche nei confronti delle società di servizi ai fini dell'applicazione delle disposizioni di vigilanza per le banche.*([35])

Secondo quanto previsto dal Decreto del Ministero dell'economia e delle finanze 21/4/2015, "*le monete denominate in euro possono essere rimesse in circolazione dai gestori del contante esclusivamente nel caso in cui abbiano superato i prescritti controlli di autenticità*" e idoneità alla circolazione delle stesse (cfr. art. 4, comma 3, del DM). Inoltre, l'art. 6, comma 3, del DM consente ai gestori del contante di esternalizzare, in tutto o in parte, ad altro gestore il trattamento di autenticazione e selezione delle monete, fermo restando l'obbligo del committente di svolgere un controllo sull'attività esternalizzata.

Le disposizioni di vigilanza definiscono l'"*esternalizzazione*" come "*l'accordo in qualsiasi forma tra una banca e un fornitore di servizi in base al quale il fornitore realizza un processo, un servizio o un'attività della stessa banca*" (cfr. Circolare n. 285 del 17 dicembre 2013, Parte Prima, Titolo IV, Capitolo 3, Sezione I). Ciò che rileva ai fini dell'individuazione di un processo di esternalizzazione è, quindi, che il fornitore svolga effettivamente un'attività di competenza della banca e per la quale essa rimane comunque responsabile.

Si ritiene quindi che l'attività di gestione delle monete nei termini sopra descritti rientri nella definizione di attività esternalizzata ai sensi delle disposizioni di vigilanza per le banche e sia quindi assoggettata alla relativa disciplina.

Si ricorda che, nel caso di esternalizzazione del trattamento del contante, il paragrafo 4 della Parte Prima, Titolo IV, Capitolo 3, Sezione IV, della Circolare n. 285/2013, prevede espressamente la stipulazione di un contratto in forma scritta nel caso in cui la banca intenda esternalizzare l'attività di trattamento del contante ai fornitori di servizi. Inoltre, il medesimo paragrafo stabilisce che la banca committente è tenuta, tra l'altro, ad adottare "*specifiche cautele nella gestione dei rapporti con i soggetti cui l'attività è esternalizzata sia all'atto della scelta del contraente […], sia nell'esercizio di efficaci controlli successivi, da svolgere nel continuo per verificare l'ordinato e corretto svolgimento dell'attività, nel pieno rispetto delle norme vigenti*".

[35] Aggiornamento del 6 febbraio 2017.

CONTROLLI DI GRUPPO (Parte Prima, Titolo IV, Capitolo 3, Sezione V)

1. *Un dipendente della controllante può essere dislocato presso la controllata in qualità di referente per la funzione di controllo esternalizzata all'interno del gruppo?* ([36])

Cfr. Resoconto della consultazione, pag. 63.

OSSERVAZIONE	VALUTAZIONE (Sì, No, In Parte, Chiarimento)	COMMENTO
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 di pendente della banca che esternalizza le funzioni di controllo.

2. *Nei casi di* compliance *accentrata presso la capogruppo, il responsabile della funzione nominato dalla capogruppo, può essere individuato tra i dirigenti/quadri della funzione di conformità? La nomina del referente presso le banche controllate può avvenire su designazione della capogruppo e questi può essere individuato tra i dirigenti/quadri della banca controllata, deputati ad attività di controllo di primo livello?* ([37])

Con riferimento al primo quesito, sia il responsabile della funzione di controllo accentrata presso la capogruppo sia il referente presso la società controllata devono essere individuati tra i soggetti che rispettino i requisiti previsti dalla Sezione III, par. 1, lett. b). L'inquadramento nell'organico aziendale deve essere tale da garantire il rispetto delle richiamate disposizioni.

Con riferimento al secondo quesito, il referente di una funzione aziendale di controllo esternalizzata non può essere identificato con il responsabile dei controlli di primo livello, in quanto ciò non sarebbe coerente con il principio in base al quale i controlli di primo e secondo livello vanno tenuti separati (cfr. Sezione I, par. 6) e con la previsione secondo cui il responsabile dei controlli di secondo livello non può avere responsabilità di aree operative (inclusi, i controlli di linea) sottoposte ai controlli (cfr. Sezione III, par. 1, lett. b).

[36] Aggiornamento del 6 giugno 2014.
[37] Aggiornamento del 6 giugno 2014.

SUCCURSALI DI BANCHE COMUNITARIE E DI BANCHE EXTRACOMUNITARIE AVENTI SEDE NEGLI STATI INDICATI NELL'ALLEGATO A DELLE DISPOSIZIONI INTRODUTTIVE (Parte Prima, Titolo V, Capitolo 3, Sezione VII)

1. *Nell'attestazione annuale del legale rappresentante sulla verifica della conformità dell'attività aziendale alle norme italiane, qual è il perimetro normativo cui fare riferimento?*

   Il perimetro normativo di riferimento include non solo tutte le disposizioni applicabili delle quali la Banca d'Italia verifica l'osservanza e riportate nella Circolare n. 285, Parte Prima, Titolo I, Capitolo 2, Sezione II, Allegato A, ma anche le altre norme italiane comunque applicabili alla succursale (quali, ad esempio, la normativa fiscale, la normativa in materia di trattamento dei dati personali, ecc.).

2. *Qual è il termine per l'invio della prima attestazione di conformità?*

   L'attestazione del legale rappresentante è trasmessa alla Banca d'Italia insieme al questionario che le succursali inviano alla Banca d'Italia entro il 30 novembre di ogni anno.

3. *In che misura le disposizioni dei capitoli 4 e 5, in materia rispettivamente di sistema informativo e continuità operativa, si applicano alle succursali di banche comunitarie e alle succursali di banche extracomunitarie aventi sede negli Stati indicati nell'Allegato A delle Disposizioni introduttive?* ([38])

   Le succursali di banche comunitarie e le succursali di banche extracomunitarie aventi sede negli Stati indicati nell'Allegato A delle Disposizioni introduttive non sono in generale soggette alle disposizioni dei capitoli 4 (Il sistema informativo) e 5 (La continuità operativa).

   Qualora tuttavia, ricorrendone i presupposti (cfr. Capitolo 5, par.1), dette succursali fossero individuate dalla Banca d'Italia quali responsabili di processi a rilevanza sistemica per l'operatività del sistema finanziario nazionale, esse sarebbero assoggettate ai pertinenti requisiti in materia di continuità operativa previsti dal Capitolo 5.

RISCHIO DI CREDITO (Parte Prima, Titolo IV, Capitolo 3, Allegato A)

1. *Nel caso in cui in una banca già esistessero strutture che effettuano un controllo di secondo livello sul monitoraggio andamentale del credito, le nuove disposizioni impongono la loro riallocazione nell'ambito del* risk management*?*

   La verifica del corretto svolgimento 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 sono svolte dal *risk management* o, per le banche di maggiore dimensione e complessità operativa, da una specifica unità, che riporta al responsabile della

[38] Aggiornamento del 6 giugno 2014.

funzione di controllo dei rischi. Ove esistessero strutture che già effettuano tali attività, ai fini del rispetto della nuova normativa queste devono essere collocate a riporto gerarchico del responsabile del *risk management*.

2. *Cosa si intende per adeguatezza delle procedure di recupero? Tale attività sembrerebbe avere degli elementi di sovrapposizione con quella tipicamente svolta dalla funzione di audit, funzione cui è istituzionalmente demandata "la verifica dell'adeguatezza e il corretto funzionamento dei processi e delle metodologie di valutazione" (cfr. Sezione III, par. 3, punto 3.4 sub e).* ([39])

   Le procedure di recupero sono adeguate se in grado di ottenere efficientemente ed efficacemente il recupero delle esposizioni secondo tempistiche, modalità e importi coerenti con il processo di gestione dei rischi.

   La valutazione di adeguatezza condotta dal *risk management* non si sovrappone a quella dell'*internal audit* : il primo concorre alla definizione del processo di recupero e verifica nel continuo che le procedure di recupero, non solo siano formalmente previste, ma anche rispettate nel concreto da parte delle unità operative; il *risk management*, pertanto, valuta l'adeguatezza operando un controllo di secondo livello svolto nel continuo e diretto non solo a identificare criticità ma anche a collaborare con le strutture preposte per l'individuazione delle azioni correttive; l'*internal audit* agisce secondo logiche di terzo livello, fornendo un giudizio di affidabilità ed efficacia complessive del processo di recupero completamente indipendente e "terzo" dalla fase operativa e di controllo di secondo livello; essa, secondo un approccio *risk based*, assicura verifiche periodiche che possono avere ad oggetto, fra l'altro, l'attività dello stesso *risk management*.

3. *La verifica del corretto svolgimento del monitoraggio andamentale deve essere espletata su ogni singola posizione? È possibile avere qualche orientamento più specifico sulla frequenza e modalità di conduzione della stessa.* ([40])

   La verifica del corretto svolgimento del monitoraggio andamentale sulle singole esposizioni deve essere effettuata dalla funzione di controllo dei rischi secondo criteri e modalità oggettivi, identificati ex ante, che non comportino la duplicazione dell'attività del monitoraggio andamentale svolto nell'ambito dei controlli di primo livello, ma siano in grado di identificare in maniera sistematica e tempestiva eventuali carenze del processo di monitoraggio. In tal senso, il *risk management* identifica almeno indicatori di *early warning* che segnalino tempestivamente anomalie del monitoraggio andamentale svolto dalla prima linea (ad es., utilizzo di perizie immobiliari non adeguatamente aggiornate, utilizzo di coefficienti di svalutazione non correlati alla durata della permanenza di una certa posizione in sofferenza, mantenimento di posizioni in incaglio senza adozione di tempestive misure correttive), in presenza dei quali procedere al controllo delle singole posizioni interessate.

[39] Aggiornamento del 6 giugno 2014.
[40] Aggiornamento del 6 giugno 2014.

FILIALI ESTERE (Parte Prima, Titolo IV, Capitolo 3, Allegato B)

1. *Il personale deputato alle attività di* compliance *presso filiali estere può essere collocato a riporto funzionale anziché gerarchico della funzione accentrata?* ([41])

Cfr. Resoconto della consultazione, pag. 71.

OSSERVAZIONE	VALUTAZIONE (Sì, No, In Parte, Chiarimento)	COMMENTO
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 principi o condivisibile delle doppie linee di riporto (c he 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 informati vo al responsabile locale e all'unità centrale.

2. *Presso le filiali estere è possibile avere un'unica struttura che espleti i controlli di secondo livello?* ([42])

La Circ. 285/2013 prevede espressamente che le banche debbano istituire presso le succursali con una significativa operatività (tenuto conto sia della rischiosità della succursale rispetto alla complessiva propensione al rischio della banca, sia della complessità operativa/organizzativa della succursale stessa) un'unità incaricata dei controlli di secondo livello e un'unità avente funzioni di revisione interna. Per le filiali estere con operatività non significativa non sono previsti obblighi specifici; ne consegue, che è rimessa all'autonomia delle banche la definizione di un assetto idoneo dei controlli della filiale.

RAF (Parte Prima, Titolo IV, Capitolo 3, Allegato C)

1. *Qual è la periodicità del RAF e come si coordina con l'ICAAP?* ([43])

La periodicità di redazione del RAF è rimessa alle banche, che valutano le eventuali esigenze di aggiornamento o modifica anche in funzione delle variazioni del contesto di mercato, del modello di *business*, del piano strategico, del processo di gestione dei rischi e delle risultanze del processo ICAAP.

Il processo ICAAP è uno dei processi aziendali tramite cui si attua e si implementa il RAF.

[41] Aggiornamento del 6 giugno 2014.
[42] Aggiornamento del 6 giugno 2014.
[43] Aggiornamento del 6 giugno 2014.

SISTEMA INFORMATIVO (Parte Prima, Titolo IV, Capitolo 4)

1. Cosa si intende per rischio residuo? ([44])

Il "rischio informatico residuo" è definito al Capitolo 4 come il rischio informatico a cui l'intermediario è esposto una volta applicate le misure di attenuazione individuate nel processo di analisi dei rischi. Il rischio valutato prima dell'applicazione di tali misure è detto rischio potenziale; si noti che quest'ultimo non coincide con la quota parte di "*risk capacity*" relativa all'ICT, che rappresenta invece il massimo rischio teoricamente sopportabile dalla banca in relazione all'utilizzo delle proprie risorse ICT.

2. Cosa si deve intendere per "componente critica" del sistema informativo? ([45])

La definizione di "componente critica del sistema informativo" è indicata nella Sezione I, par. 3, in rapporto alle conseguenze di un'eventuale incidente di sicurezza informatica per il regolare e sicuro svolgimento di funzioni operative importanti. Come si evince dalla stessa definizione, l'intermediario a partire dalle proprie funzioni operative importanti (così come definite nel Capitolo 3, Sezione I, par. 3), individua, attraverso l'analisi dei rischi, le componenti del sistema informativo che supportano o comunque svolgono un ruolo cruciale per la sicurezza delle menzionate funzioni operative importanti.

3. Le Raccomandazioni BCE sulla sicurezza dei pagamenti internet richiamate nelle disposizioni normative della Banca d'Italia, richiedono in generale l'autenticazione forte dell'utente ("strong customer authentication*") per l'autorizzazione di disposizioni di pagamenti via internet nonché per l'accesso a "dati sensibili di pagamento" (*Recommendation *7). Quali criteri possono essere adottati per verificare la conformità di una soluzione di autenticazione a questo requisito? È comunque possibile applicare il principio del "*comply or explain*"?* ([46])

Le Raccomandazioni BCE includono una definizione di "*strong customer authentication*" (cfr. *Guiding principles*, pag. 3); in particolare, oltre alla tradizionale combinazione di elementi (o fattori) di tipo diverso e ad eccezione del caso di adozione del tipo "inerente", sono richieste ulteriori caratteristiche quali la non replicabilità e la non riusabilità del codice di autenticazione generato per almeno un elemento. Per approfondire i requisiti che deve soddisfare una soluzione di "*strong customer authentication*" si rimanda all'"*Assessment Guide for the security of internet payments*" pubblicata dalla BCE il 4/2/2014.

Il principio del "*comply or explain*" si applica alle previsioni contenute nelle "*Recommendations for the security of internet payments*" della BCE e quindi anche al requisito di "*strong authentication*". In particolare, l'intermediario può non applicare talune "*Recommendations*" o "*Key Considerations*", fornendo opportune spiegazioni e giustificazioni che siano soddisfacenti per l'autorità di vigilanza. Tali giustificazioni devono essere basate su un'analisi dei rischi approfondita e documentata.

[44] Aggiornamento del 6 giugno 2014.
[45] Aggiornamento del 6 giugno 2014.
[46] Aggiornamento del 6 giugno 2014.

CONTINUITÀ OPERATIVA (Parte Prima, Titolo IV, Capitolo 5)

1. *Quali sono i destinatari della normativa di cui al Capitolo 5, Allegato A, Sezione II (Requisiti per tutti gli operatori)?* ([47])

   Le disposizioni del Capitolo 5, Allegato A, Sezione II (Requisiti per tutti gli operatori) si applicano:

   - alle banche autorizzate in Italia, ad eccezione delle succursali di banche extracomunitarie aventi sede negli Stati indicati nell'Allegato A delle Disposizioni introduttive;
   - alle capogruppo di gruppi bancari;
   - alle imprese di riferimento, secondo quanto previsto dalla Sezione VI del Capitolo 3.

2. *Nel par. 3 è stabilito che la capogruppo di un gruppo bancario assicuri che tutte le controllate siano dotate di piani di continuità operativa. Tale requisito si intende applicabile solo ed esclusivamente alle banche o anche alle altre società che compongono il gruppo? In ogni caso, l'ambito di applicazione è indipendente dalla criticità e/o settore di attività oppure valgono i principi definiti all'interno del RAF in merito alla rischiosità per stabilire se una società debba o meno essere dotata di un piano di continuità?* ([48])

   Il perimetro di applicazione si intende esteso a tutte le società che compongono il gruppo e non è quindi limitato alle società bancarie. L'adozione o meno di un piano di continuità operativa per tutte le società del Gruppo dipende dalla criticità dei processi gestiti dalle stesse società. Compete alla capogruppo definire metriche comuni di valutazione dei rischi operativi per tutte le società del gruppo (cfr. Capitolo 3, Sezione III, par. 3.3 ([49]) e Sezione V). A valle di un'analisi di impatto dei processi aziendali gestiti (cfr. Allegato A, Sezione II, par. 3), condotta sulla base di linee guida emanate dalla capogruppo, può emergere la necessità di predisporre soluzioni di continuità operativa.

   Inoltre, sulla base di quanto stabilito al Capitolo 3, Sezione V, par. 2 (Controlli interni di gruppo ([50]), si evince che, con riferimento alla gestione della continuità operativa, indipendentemente dal modello accentrato o decentrato adottato per il piano (cfr. par. 3), è sempre la capogruppo che, oltre a definire linee guida comuni, svolge attività di controllo al fine di assicurare la corretta applicazione di metriche omogenee di

---

[47] Aggiornamento del 6 giugno 2014.
[48] Aggiornamento del 6 giugno 2014.
[49] Secondo cui: "*La funzione di controllo dei rischi:…definisce metriche comuni di valutazione dei rischi operativi coerenti con il RAF, coordinandosi con la funzione di conformità alle norme, con la funzione ICT e con la funzione di continuità operativa*".
[50] Secondo cui: "*La capogruppo, nel quadro dell'attività di direzione e coordinamento del gruppo esercita: c) un controllo tecnico-operativo finalizzato alla valutazione dei vari profili di rischio apportati al gruppo dalle singole controllate e dei rischi complessivi del gruppo."; e, inoltre, "Per definire il sistema dei controlli interni del gruppo bancario, la capogruppo applica, per quanto compatibili, le disposizioni previste nelle precedenti Sezioni. A livello di gruppo – tenendo conto delle disposizioni in materia di organizzazione e controllo dei soggetti diversi dalle banche – vanno anche stabiliti e definiti:…-controlli sul raggiungimento degli obiettivi di sicurezza informatica e di continuità operativa definiti per l'intero gruppo e le singole componenti.*"

valutazione dei rischi e garantire la coerenza nei risultati (ad es. due processi analoghi gestiti da due distinte società del gruppo non possono essere valutati con un differente livello di criticità).

3. *La capogruppo di un gruppo bancario deve essere coinvolta nella definizione dei piani e delle soluzioni di continuità operativa delle controllate o può essere sufficiente che definisca delle linee guida cui le società controllate devono attenersi?* ([51])

   La capogruppo deve assicurarsi che tutte le società controllate siano dotate di piani di continuità operativa coerenti con gli obiettivi strategici del gruppo in tema di contenimento dei rischi. Nel rispetto di tale obbligo, la capogruppo può anche non essere coinvolta nella fase di redazione del piano di continuità operativa.

4. *Con quali modalità ed entro quale termine deve essere comunicato il responsabile del piano di continuità operativa?* ([52])

   La comunicazione del responsabile del piano di continuità operativa è effettuata mediante la procedura GIAVA – OR.SO. (organi sociali), accessibile all'indirizzo https://www.bancaditalia.it/statistiche/raccolta-dati/segnalazioni/rilevazioni-vigilanza/index.html.

   Nel caso di responsabili del piano designati prima dell'entrata in vigore delle nuove disposizioni, va convenzionalmente indicata la decorrenza dal 2 luglio 2013 (date anteriori non sono accettate dalla procedura).

   Il termine ultimo per la comunicazione è fissato al 1° luglio 2014 (data di efficacia delle disposizioni contenute nel Capitolo 5).

   Nel caso di gruppi bancari, l'indicazione del responsabile del piano di continuità operativa è fornita per tutte le banche appartenenti al gruppo; nel caso in cui il piano sia definito e gestito in modo accentrato per l'intero gruppo, deve essere replicato per ogni società del gruppo il nominativo del responsabile del piano presso la capogruppo.

[51] Aggiornamento del 6 giugno 2014.
[52] Aggiornamento del 6 giugno 2014.